NIST Internal Report
NIST IR 8467 2pd

Genomic Data Cybersecurity and Privacy Frameworks Community Profile

Second Public Draft

Ronald Pulivarti
Justin Wagner
Justin Zook
Eugene Craft
Brett Kreider
Jeremy Miller
Patrick O'Neil
Christina Sames
Julie Snyder
Bob Stea
Martin Wojtyniak

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8467.2pd

NIST
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Internal Report
NIST IR 8467 2pd

Genomic Data Cybersecurity and Privacy Frameworks Community Profile

Second Public Draft

Ronald Pulivarti
National Cybersecurity Center of Excellence
Information Technology Laboratory

Justin Wagner
Justin Zook
Biosystems and Biomaterials Division
Material Measurement Laboratory

Eugene Craft
Brett Kreider
Jeremy Miller
Patrick O'Neil
Christina Sames
Julie Snyder
Bob Stea
Martin Wojtyniak
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8467.2pd

December 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Technical Series Policies

How to Cite this NIST Technical Series Publication

Pulivarti R, Wagner J, Zook J, Craft E, Kreider B, Miller J, O’Neil P, Sames C, Snyder J, Stea B, Wojtyniak M (2024) Integrated Genomic Data Cybersecurity and Privacy Framework Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR (Internal Report) NIST IR 8467 2pd. https://doi.org/10.6028/NIST.IR.8467.2pd

Author ORCID iDs

Ronald Pulivarti: 0000-0002-8330-3474
Justin Wagner: 0009-0003-8903-0504
Justin Zook: 0000-0003-2309-8402
Eugene Craft: 0009-0009-0164-1241
Brett Kreider: 0009-0004-1508-5876
Jeremy Miller: 0009-0004-3119-8803
Patrick O’Neil: 0009-0004-7313-1201
Christina Sames: 0009-0003-1817-8333
Julie Snyder: 0009-0004-6352-2831
Bob Stea: 0009-0000-0514-7085
Martin Wojtyniak: 0009-0005-9643-2194

Public Comment Period

December 16, 2024 – January 30, 2025

Submit Comments

genomic_cybersecurity_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information

Additional information about this publication is available at the NCCoE's Cybersecurity and Privacy of Genomic Data project page, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Advancements in genomic sequencing technologies are accelerating the speed and volume of data collection, sequencing, and analysis. However, this progress also heightens cybersecurity and privacy risks. This Genomic Data Cybersecurity and Privacy Frameworks Community Profile ("Genomic Data Profile") identifies the priority outcomes from both the Cybersecurity Framework (CSF) and the Privacy Framework (PF) to provide guidance to reduce cybersecurity and privacy risks to organizations in the genomic data life cycle. This updated version includes both cybersecurity based on the CSF 2.0 and privacy based on the PF 1.0. In developing this Profile, NIST worked closely with genomic stakeholders across government, industry, and academia to identify cybersecurity and privacy risks and priorities.

Keywords

bioeconomy; Community Profile; Cybersecurity Framework Profile; DNA sequencing; genomic data; genomic sequencing; genomics; human genome; informed consent; Privacy Framework Profile.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Supplemental Content

Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified; see the NIST IR 8467 (draft) publication details.

Note to Reviewers

NIST welcomes feedback and input on any aspect of this publication. Specifically, NIST seeks feedback on:

1. How well do the practices in this publication relate to existing practices and standards leveraged by your organization? Are there significant gaps between the sets of practices that this publication should address? Would mappings to other standards and guidelines be useful or do mappings already exist that you use?

2. How do you expect this publication to influence your future practices and processes? Are there specific guidance documents or best practices that you recommend? For example, NIST published CSF 2.0 implementation examples to show potential ways to achieve the outcome in each Subcategory. What genomics-specific implementation examples would be valuable? What scenarios for cybersecurity and privacy threat modeling and mitigations would be valuable?

3. How do you envision using this publication? What changes would you like to see to increase/improve that use?

4. What suggestions do you have on changing the format of the information provided?

5. Is the guidance in this document sufficient to help your organization prioritize cybersecurity and privacy outcomes?

Commenters are encouraged to use the comment template provided on the NCCoE's Cybersecurity and Privacy of Genomic Data project page for responses to the question set and for specific comments on the text of the document. Please submit your feedback and completed comment templates to the project team at genomic_cybersecurity_nccoe@nist.gov. The deadline to submit comments is **11:59 p.m. Eastern Time on January 30, 2025**.

All comments are subject to release under the Freedom of Information Act.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: genomic_cybersecurity_nccoe@nist.gov

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors would like to acknowledge all those that contributed to the development of this report, including:

- Cherilyn Pascoe, NIST
- Dylan Gilbert, NIST
- Naomi Lefkovitz, NIST
- Sheng Lin-Gibson, NIST
- Jennifer McDaniel, NIST
- Theresa Suloway, MITRE
- Hillary Tran, MITRE
- Spike E Dog, MITRE
- Faith Ryan, MITRE
- Karen Scarfone, Scarfone Cybersecurity
- Jorge Acevedo Canabal, University of Puerto Rico School of Medicine
- David Bernick, Broad Institute
- Katherine Blizinsky, PhD, National Institutes of Health
- Whitney Bowman-Zatzkin, Bioeconomy Information Sharing and Analysis Center
- E. Loren Buhle, Jr. PhD, DNAnexus Inc.
- Senthil Gurumoorthi, Amazon
- Jean-Pierre Hubaux, EPFL and Tune Insight, Switzerland
- Gail P. Jarvik, M.D., Ph.D., University of Washington Medical Center, Seattle WA
- Roberto Lleras, Microsoft Research
- Oki Mek, Microsoft Federal Civilian
- Tommy Morris, The University of Alabama in Huntsville
- Paul Murdock, Roche Diagnostics International
- Bill Reid, MS, FACHE, FIP, CISM, Google Cloud’s Office of the CISO
- John Signorino, JD MHSA, Mayo Clinic
- Carrie Smedira, Microsoft
- Justin Trimachi, JD, CIPP/E, CIPP/US, CIPM, LabCorp
- Timothy J. Walsh, CISSP, CSSLP, Mayo Clinic
- Phillip Whitlow, HudsonAlpha Institute for Biotechnology
- Ken Wiley, Jr. Ph.D., National Center for Advancing Translational Sciences

Executive Summary

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) engaged stakeholders across government, academia, and industry to better understand the current state of the cybersecurity and privacy challenges facing the genomics community. This collaboration led to NIST publishing NIST Internal Report (IR) 8432, *Cybersecurity of Genomic Data*, an overview of the challenges and opportunities with genomic data cybersecurity. As a follow-on effort, the NCCoE collaborated with a diverse subset of stakeholders to conduct working sessions focused on gathering the information needed to develop this *Genomic Data Cybersecurity and Privacy Frameworks Community Profile* (referred to as the "Genomic Data Profile"). This Profile prioritizes Subcategories from the Cybersecurity Framework (CSF) 2.0 and the Privacy Framework (PF) 1.0 in a single integrated Profile for the genomic community.

The Genomic Data Profile provides guidance to help organizations manage and reduce cybersecurity and privacy risks for assets[1] that process any type of genomic data (e.g., human, microbiome, microbial, model organism, plant) as well as privacy risks to individuals whenever human genomic data is processed. The Profile is intended to help organizations understand, assess, prioritize, and communicate their existing and future cybersecurity and privacy strategies, priorities, activities, practices, policies, and guidance. Organizations consider their unique obligations, operating environment, and Mission Objectives when prioritizing and implementing cybersecurity and privacy capabilities.

This Profile identifies 12 genomic-related Mission Objectives and prioritizes relevant Subcategories to help organizations protect genomic data and individuals throughout the data life cycle. CSF and PF Subcategories describe the relevant outcomes from implementing cybersecurity and privacy capabilities. Prioritizing cybersecurity and privacy capabilities based on their organization's Mission Objectives can inform decision-making.

The selection of cybersecurity and privacy capabilities for genomic data is complicated by the broad and diverse nature of the genomics community, including biopharmaceutical research, healthcare, law enforcement, and agriculture. Organizations rely on genomic data sharing to advance scientific and medical research, improve health outcomes, and compete within the bioeconomy, and thus genomic data often needs to be aggregated from multiple sources. In addition, organizations that share data with stakeholders in multiple countries may have additional requirements for protecting genomic data or for managing the cross-border transfer of data.

Cybersecurity attacks targeted at assets that process genomic data could impact the confidentiality, integrity, and availability of that data, introducing economic, privacy, discrimination, and national security risks. Additionally, processing human genomic data can impact the predictability, disassociability, and manageability of that data, which may result in privacy risks to individuals. For example, the unanticipated revelation of genomic data may

[1] The CSF 2.0 uses the term asset to describe "assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes" (ID.AM).

result in an individual's loss of trust and autonomy when working with a particular organization and cause them to opt out of future activities that would benefit them or a broader population (e.g., research or treatments).

Organizations processing any type of genomic data can use this Profile to:

- Understand cybersecurity and privacy considerations for genomic data
- Assess current organizational cybersecurity and privacy practices to identify gaps and areas of improvement for existing practices or infrastructure
- Develop individualized Organizational Target (To-Be) Profiles
- Prioritize investments in cybersecurity and privacy capabilities aligned to the Subcategories identified as most important to support organizational Mission Objectives
- Understand the relationship between cybersecurity and privacy risk management

1. Introduction

The NIST Cybersecurity Framework (CSF) [1] and Privacy Framework (PF) [2] provide guidance to help organizations manage cybersecurity and privacy risks. The Frameworks were created through collaboration with a diverse range of stakeholders and encourage a prioritized, risk-based approach to address cybersecurity and privacy issues. Although the Frameworks present a variety of mitigations, there are also Community Profiles, such as the one defined in this document, that tailor and prioritize those mitigations for a specific sector, industry, or other use case.

The NIST NCCoE engaged stakeholders from government, academia, and industry to better understand the current state of the cybersecurity and privacy challenges facing the genomics community. In 2022, the NCCoE conducted two public workshops—the first concentrating on the challenges faced or anticipated by the community [3] and the second focusing on solutions to help address those challenges [4]. NIST published NIST Internal Report (NIST IR) 8432, *Cybersecurity of Genomic Data* [5], to further explore and document the concepts identified in the workshops, including the concerns and challenges associated with processing genomic data, the current state of relevant cybersecurity risk management practices[2], gaps in implementing genomic data protections, and potential solutions along with areas for further research. NIST IR 8432 can be used as a supplement to this document, providing context and background for a better understanding of the current state of cybersecurity practices when processing genomic data.

As a follow-on effort, the NCCoE collaborated with a diverse subset of these stakeholders to conduct working sessions designed specifically to identify cybersecurity and privacy priorities to generate the information needed to develop this integrated Genomic Data Profile. This Profile uses the CSF version 2.0 and PF version 1.0, the current versions at time of publication.

1.1. Purpose

This Genomic Data Profile provides guidance to help organizations manage cybersecurity and privacy risks for assets that process genomic data. The Profile helps organizations prioritize cybersecurity and privacy capabilities based on their Mission Objectives, which can inform cybersecurity and privacy decision-making. The Profile is intended to help organizations organize and communicate their existing and future cybersecurity and privacy activities, practices, policies, and guidance. Organizations should consider their own obligations, operating environment, and Mission Objectives when prioritizing and implementing cybersecurity and privacy capabilities.

The selection of cybersecurity and privacy capabilities for genomic data is complicated by the broad and diverse nature of the genomics community, including biopharmaceutical research, basic science research, healthcare, law enforcement, and agriculture. Cyber-attacks targeted at assets that process genomic data could impact the confidentiality, integrity, and availability of that data, introducing economic, privacy, discrimination, and national security risks.

[2] The focus of the workshops was on cybersecurity, but many participants noted the importance of privacy, too.

Additionally, processing human genomic data can impact the predictability, disassociability, and manageability of that data, which may result in privacy risks to individuals. For example, the unanticipated revelation of genomic data may result in an individual's loss of trust and autonomy when working with a particular organization and cause them to opt out of future activities that would benefit them or a broader population (e.g., research or treatments). This Profile integrates cybersecurity and privacy guidance, acknowledging the intersection of cybersecurity with privacy (see Sec. 2.3).

Organizations processing genomic data can use this Profile to:

- Understand cybersecurity and privacy considerations for genomic data
- Assess current organizational cybersecurity and privacy practices to identify gaps and areas of improvement for existing practices or infrastructure
- Develop individualized Organizational Target (To-Be) Profiles
- Prioritize investments in cybersecurity and privacy capabilities aligned to the Subcategories identified as most important to support organizational Mission Objectives
- Understand the relationship between cybersecurity and privacy risk management

Legislation such as the Genetic Information Nondiscrimination Act of 2008 (GINA)[3] expands the need to protect genetic data, while Executive Order (EO) 14081[4] [6] lays out the need to identify risks and develop a protection plan for biological datasets, including genomic data. The EO seeks to implement a whole-of-government approach for bolstering biotechnology and biomanufacturing, which includes advancing a biological data ecosystem that spurs innovation while adhering to security and privacy standards. The EO directs the Secretary of Homeland Security, in coordination with the Secretary of Commerce (acting through the Director of NIST) and other government agencies, to identify and recommend cybersecurity best practices for biological data stored on Federal Government information systems.

Genomic data is one form of multipurpose, high-value biological data used by Federal Government agencies as well as the private sector. Section 4 of the EO calls for establishing a "Data for the Bioeconomy Initiative (Data Initiative)" that will identify data types and sources critical to the bioeconomy. The EO addresses genomic data, its role in the bioeconomy, and the need to develop data protection plans that address security, privacy, and risks to this data and other related data types. This Profile serves as one source for identifying and recommending cybersecurity and privacy best practices for protecting genomic data, which may also apply to other biological data types.

1.2. Scope

Genomic information is possessed by all living organisms, including humans. When extracted, this information exists in different forms throughout its life cycle, which may include the

[3] The Genetic Information Nondiscrimination Act of 2008 (GINA) is a U.S. congressional law that protects individuals against discrimination on the basis of genetic information in health coverage and in employment.

[4] EO 14081, Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy, was issued on September 12, 2022

following phases: sample collection, sample preparation, data generation, data analysis, and data disposition. Fig. 1 illustrates this life cycle, identifying the primary scope for this Profile to be genomic data generated via sequencing or other techniques, in yellow, with data generated by subsequent analyses, in blue.

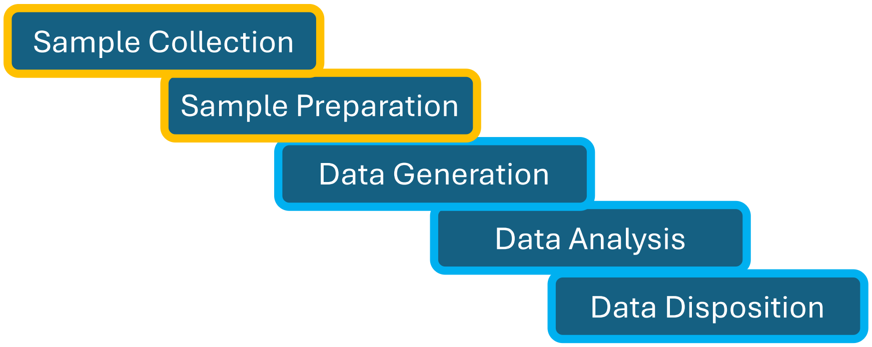


Fig. 1. Genomic Data Life Cycle Phases [7]

Organizations processing human genomic data consider the privacy protections not only of donors, but also relatives, whose privacy may be impacted because of the unique and lasting potential for identifying individuals and their relatives through deoxyribonucleic acid (DNA) samples. When human genetic material is processed, the sample preparation, data generation, and data analysis phases can be subject to privacy considerations, such as notice and informed consent, which are initially addressed before sample collection. Due to the impact of these privacy considerations on the steps that are in scope, this Profile also includes guidance for integrating outcomes from the privacy-related processes that are initiated during earlier phases in the genomic data life cycle.

1.3. Audience

The intended audience for this Genomic Data Profile is organizations that process genomic data, including sequencing service providers, genome centers, clinical laboratories, healthcare organizations, direct-to-consumer test providers, sequencing technology developers, and cloud platform providers for genomic data processing. This Profile can be used by these organizations to identify and communicate cybersecurity and privacy expectations with internal and external parties, such as leadership, cybersecurity and privacy staff, and others who architect and monitor genomic data processing workflows.

While the audience members will likely have a technical background, this document does not assume readers have extensive cybersecurity or privacy experience. As such, the background provided in Sec. 3 helps make this document self-contained for all audiences but may be skimmed by those with more familiarity with the CSF and PF.

1.4. Document Structure

This document is organized into the following sections:

- Section 2 provides an overview of genomic data and a description of the relationship between cybersecurity and privacy.
- Section 3 introduces the NIST Cybersecurity and Privacy Frameworks, including information on Community Profiles and their application.
- Section 4 describes the methodology used to develop this Profile.
- Section 5 identifies genomics community organizational Mission Objectives and their prioritization.
- Section 6 provides the prioritized Subcategories for each Mission Objective and the rationale for prioritization.
- The References section contains cited resources.
- Appendix A includes links to NIST Framework resources, Appendix B includes a list of acronyms and abbreviations, and Appendix C includes a glossary of terms.
- A spreadsheet version of the prioritized Subcategories is available at the NCCoE’s Cybersecurity and Privacy of Genomic Data project page.

2. Overview of Genomic Data

The genome is the complete set of genetic instructions to form an organism. These instructions are encoded in the sequence of bases that comprise the DNA molecule: adenine (A), cytosine (C), guanine (G), and thymine (T). Genes are the functional units of the genome. They contain instructions for making products that carry out essential functions in a cell, like proteins. Genes vary in size and complexity. The human genome contains approximately 3.1 billion base pairs encoding about 20,000 genes, most of which are uncharacterized. Paris japonica, a flowering plant native to Japan, has the largest recorded genome to date, approximately 50 times larger than the human genome. The stretches of DNA that lie between genes are known as intergenic, or non-coding, regions. Intergenic regions contain elements that regulate gene activity and make up the majority of the human genome. The genome plays a central role in heritability, the passing of traits from parents to offspring, as it carries the genetic information that determines these traits. Though mutations occasionally occur, the genome is stable and faithfully passed down from generation to generation.

Genomic data are generated from studying the structure and function of an organism's genome, which consists of genes and other elements that control the activity of genes. Examples of genomic data can include the DNA sequence, sequence variants, modifications, gene activity, and annotations such as gene names, functions, and standardized gene ontology identifiers. A key method that researchers use to collect and understand genomic information is DNA sequencing. Once DNA is collected and prepared for analysis, a DNA sequencer can be used to determine the order of the four bases in a given sample. The output, known as a "read," represents the string of bases identified. Sequencers differ in their methodologies, read lengths, and data quality. Currently, many sequencing platforms produce reads 150-300 bases in length. The recent development of long-read and ultra-long read technologies allows for generating reads of over 10,000 and 100,000 base pairs, respectively. For many analyses, after sequencing, reads are assembled into larger sequences called contigs. The average number of times a specific position in the genome aligns with a reference is known as "coverage.” Greater coverage improves confidence in the quality of assembled contigs and base-call accuracy by identifying sequencing errors.

The resulting file sizes from whole genome sequencing can range from tens to hundreds of gigabytes. In contrast, exome sequencing, which targets only coding regions, generates considerably smaller file sizes. Organizations may store data files locally or in public repositories to ensure transparency and scientific validity, especially when associated with published research. While sensitive data are protected to maintain privacy, researchers typically provide access to peer reviewers during the review process. Additionally, they may share data with other researchers upon request. Organizations may store genomic data in secure, high-capacity data storage systems, such as cloud-based platforms or dedicated data centers.

Genomic data has a wide range of applications across many fields. In agriculture, genomic data enable the identification of plants and animals with desirable traits, optimize approaches to feeding and nutrition based on population characteristics, and develop new or enhanced food products that resist adverse conditions or have improved nutritional profiles. In medicine and science, clinicians can use genomic information to diagnose genetic disorders, identify individuals at risk of developing certain conditions, predict disease progression, and tailor treatments to a patient's specific genetic profile. Researchers use genomic data to study populations and to understand how genes influence health, disease, and evolution in humans and across many model organisms. Pharmaceutical and biopharmaceutical companies use genomic information to identify and develop potential drug treatments and estimate the prevalence of disease markers in a population. Genomic analyses have also enabled forensic scientists to develop methods for identifying individuals from their DNA profile with a high degree of accuracy. Consumers also use genomic information to trace their ancestry or learn about certain aspects of their health without involving a healthcare provider.

Genomic data, like all sensitive information, can be at risk of being intercepted, corrupted, overwritten, misused, or deleted at each stage in its life cycle. The impacts of these risks span all forms of genomic information. Examples of cybersecurity issues may include compromising the security objectives of confidentiality (leaking of institutional or personal data), integrity (providing false or inconclusive results), and availability (rendering devices, processes, services, or facilities unavailable). Examples of privacy issues may include compromising the privacy objectives of predictability (using data for unspecified purposes), manageability (generating inaccurate information that cannot be confidently corrected), and disassociability (exposing connections between individuals and their data during authorized processing). Human genomic information is unique to an individual and can reveal a great deal of personal information, such as physical traits and susceptibility to health conditions. Each individual’s genomic profile is unique and can be used to re-identify an individual, even when measures have been taken to deidentify their data. Additionally, a person's genomic profile can be used to make inferences about their biological relatives, as close relatives share a significant portion of their DNA. Unlike many other forms of sensitive data, DNA is nearly immutable, which creates a permanent, traceable record. These considerations require a careful balancing act that establishes safeguards for protecting individual privacy and ensuring trust while promoting scientific advancement across the bioeconomy.

2.1. The Genomic Data Ecosystem and Bioeconomy

The term *bioeconomy* describes the economic activity derived from the life sciences, particularly in the areas of biotechnology and biomanufacturing, and includes industries, products, services, and the workforce [8]. The bioeconomy spans multiple public and private sectors, including academia, associations or nonprofits, governmental agencies, industry, and data subjects. Individuals and organizations in these sectors operate across multiple industries, including healthcare, research and development, agriculture, law enforcement, genealogy, manufacturing, and direct-to-consumer services. Although the boundaries of the bioeconomy are not always clear, activities that use natural resources—but not biological products—are typically not part of the bioeconomy. Genomic data is a critical asset that supports the bioeconomy.

The complex genomic data ecosystem includes a variety of individuals and organizations from the sectors participating in the bioeconomy. Participants in the genomic data ecosystem may play one or more roles in generating, curating, and/or analyzing genomic data to support operations or make decisions. Examples in which genomic data factor into the ecosystem include but are not limited to:

- Sequencing service providers who generate data for customers
- Research institutes generating or using genomic data for fundamental or biomedical research
- Biotechnology and pharmaceutical industry generating or analyzing genomic information to research a disease or develop therapeutics
- Cloud service providers storing, transferring, or providing capabilities to analyze genomic data
- Law enforcement agencies using genomic data for identification purposes
- Healthcare providers generating and using genomic information to diagnose or treat health conditions
- Public repositories housing reference data for analyses

The genomic data ecosystem continues to evolve and expand as new technologies and applications are developed. For example, healthcare providers and biomedical researchers will increasingly be able to tailor treatments to individual genetic profiles by leveraging detailed genomic information. Advancements in artificial intelligence tools will democratize complex genomic analyses, making these powerful insights accessible to a broader range of stakeholders. Capability enhancement and additional use cases also underscore existing concerns, such as maintaining the balance between data sharing and privacy, supporting interoperability across platforms and datasets while maintaining security, and managing large data files.

2.2. Cybersecurity and Privacy Risk Relationship

Cybersecurity and privacy are independent and separate disciplines. However, as shown by the Venn diagram in Fig. 2, Cybersecurity and Privacy Risk Relationship, some of their objectives do overlap and are complementary. Cybersecurity programs are responsible for protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) to provide confidentiality, integrity, and availability of data. In addition, these programs ensure organizations comply with applicable cybersecurity requirements. Privacy programs are responsible for managing the risks to individuals associated with data processing throughout the information life cycle[5] to provide predictability, manageability, and disassociability[6] of data, as well as ensuring organizations comply with applicable privacy requirements. Fig. 2 illustrates this relationship between cybersecurity and privacy risks, showing both where they overlap and where they are distinct.

[5] The information life cycle includes creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as “processing”) of data that may impact privacy.

[6] Definitions for predictability, manageability, and disassociability, which are privacy engineering objectives, can be found in the NIST Privacy Framework [2].

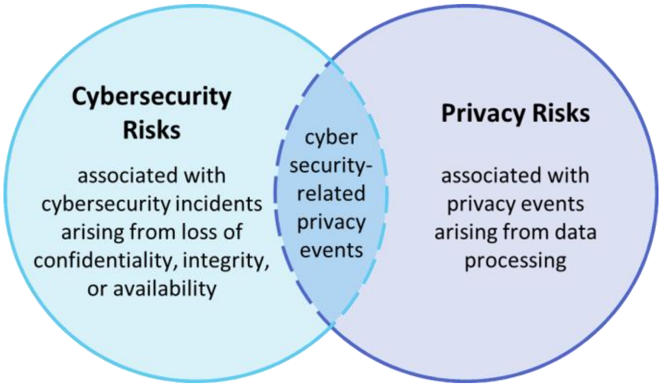

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Fig. 2. Cybersecurity and Privacy Risk Relationship [2]

While the overlap between cybersecurity and privacy risk management is important, the distinction between the two is also critical to understand. Managing cybersecurity risk contributes to managing privacy risk (e.g., controlling access to data protects against privacy breaches by limiting who can access data and the actions they can perform), but managing cybersecurity risk alone is not sufficient, as permitted data processing activities can introduce privacy risks that are unrelated to cybersecurity incidents. Some data processing activities and technologies inherently introduce privacy risks but may be necessary for valid business purposes. These privacy risks must be managed when they arise.

For example, genomic data that has been stripped of related metadata may be combined with data from other sources, such as genealogical databases or public records. Additionally, genomic data might be combined with other contextual information, such as an associated hospital, geolocation information, or medical condition. Activities like these that combine genomic data with other data can result in information that exposes a donor’s identity. While there may be many valid reasons to combine data from multiple sources, doing so can lead to the re-identification of donors. This does not mean that genomic data should not be combined with other data. Rather, it means that when this capability is provided, organizations should be aware of and manage the privacy risk introduced accordingly.

This integrated Genomic Data Profile combines the CSF and PF into a comprehensive tool that can be used to address both cybersecurity and privacy considerations for processing genomic data.

2.2.1. Privacy Risk Management Overview

Privacy risk can impact both individuals (donors or their kin) and organizations, including genomic data programs. Managing privacy risks requires genomic data programs to understand and apply privacy risk management concepts. Members of the genomic data community who are in roles that can impact privacy should also have a clear understanding of how to identify and address privacy risks that may arise during the performance of their role(s).

The NIST PF is a tool to help organizations manage privacy risk. Just as genomics programs consider the risks associated with cybersecurity incidents, they should also consider privacy events (i.e., the occurrence or potential occurrence of problematic data actions[7]). Privacy events can occur at any point throughout the genomic data life cycle, from sample collection through to data disposal. The privacy events that occur at an organization or in a system can lead to a variety of potential privacy problems that individuals experience. The PF describes privacy problems as ranging from dignity-type effects (such as embarrassment or stigmas) to more tangible harms such as discrimination, economic loss, or physical harm.[8] Privacy problems can arise from a donor's interaction with a genomics capability. Some problems can also arise for donors and relatives simply from their information being processed by genomics systems, products, and services, even when the data being processed is not directly linked to identifiable individuals. Privacy problems may also arise as consequences of activities that were implemented to provide other benefits (e.g., analyzing environmental DNA in wastewater for disease indicators).

A genomic data program may experience impacts that are a result of its role in contributing to privacy risks to individuals, such as noncompliance costs, revenue loss arising from customer abandonment of products and services, or harm to its external reputation or internal culture as a result of the privacy problems individuals may experience. Organizations typically manage these types of program impacts at the enterprise risk management level; by connecting problems that individuals experience to these well-understood program and organizational impacts, organizations can bring privacy risk into parity with other risks they are managing in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs. Fig. 3 illustrates this relationship between privacy risk and organizational risk.

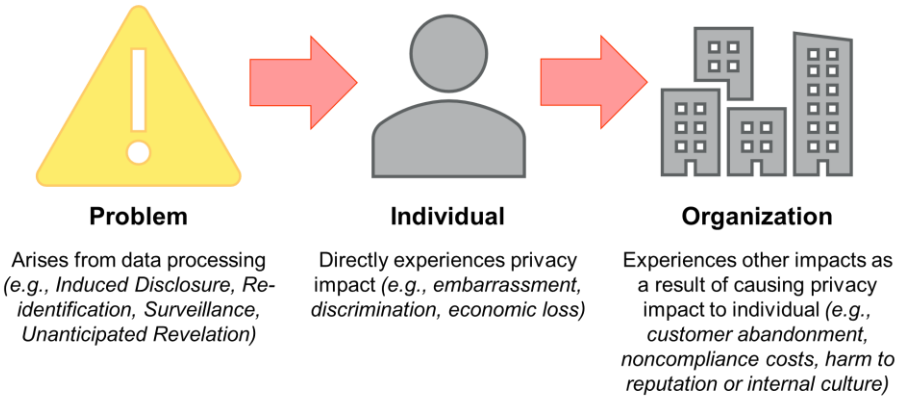

Problem
Arises from data processing (e.g., Induced Disclosure, Re-identification, Surveillance, Unanticipated Revelation)
Individual
Directly experiences privacy impact (e.g., embarrassment, discrimination, economic loss)
Organization
Experiences other impacts as a result of causing privacy impact to individual (e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

Fig. 3. Relationship Between Privacy Risk and Organizational Risk[9]

[7] A problematic data action is a data action or data processing activity that could cause an adverse effect for individuals.

[8] NIST published the *Catalog of Problematic Data Actions and Problems* to provide examples that help organizations understand and label the ways data processing activities can impact privacy ("problematic data actions") and lists problems that individuals could experience as a result. The catalogue is available at: PrivacyEngCollabSpace/catalog-PDAP.md at master · usnistgov/PrivacyEngCollabSpace · GitHub.

[9] Adapted from the NIST PF Figure 3. Catalog of Problematic Data Actions and Problems [2].

2.3. Genomic Data Security and Privacy Concerns and Challenges

Understanding the different origins of cybersecurity and privacy risks enables programs processing genomic data to effectively manage both areas of risks in the systems and services they design. NIST developed both the CSF and the PF to help organizations manage cybersecurity and privacy risks. These two frameworks are designed to be used together to assist organizations with managing the full range of cybersecurity and privacy risks. This integrated Genomic Data Profile presents the combined content of both Profiles in a single document to help organizations manage both cybersecurity and privacy risks for genomic data.

Processing any type of genomic data often includes sharing and aggregation from multiple sources to advance scientific and medical research, improve health outcomes, and compete within the bioeconomy. Processing human genomic data requires cybersecurity and privacy protections to address the unique challenges with human genomic data, such as following transparent data processing practices, managing data in accordance with differing preferences and levels of consent expressed by the subjects, and providing adequate technological and policy controls to mitigate privacy problems[10], such as discrimination or loss of trust. These protections also need to ensure data processing needs are met in a responsible manner. Responsible data sharing and analytics facilitate commerce, technological development, and research while protecting cybersecurity and privacy.

Examples of types of concerns for organizations and individuals that may arise from cybersecurity and privacy risks associated with processing human genomic data include:

- **Economic concerns** for the bioeconomy include intellectual property (IP) infringement due to exfiltration of genomic data or operational disruption due to the loss of availability of sequencing or processing services for genomic data.
- **Quality and patient safety concerns** may result from data provenance and integrity issues. Using data that cannot be trusted or lacking traceability may result in products that are harmful or ineffective, which can also erode the trust in the bioeconomy.
- **Re-identification and consent concerns** can arise from the inherent value, individuality, and immutable nature of genomic data. As the use of genomic data expands, the value of a person's genomic data increases. Potential problems from the immutability of one's own DNA, genetic similarities with relatives, and the ability to trace individuals from even partial genomic datasets increase these concerns. Even without the identifying metadata, genetic fragments may be re-identified when combined with available datasets, such as ancestry data, self-shared identified genomic data of distant relatives, surname inference, and age [7][9][10][11]. Identified or re-identified human genomic data can result in emotional distress or discrimination from revelations about disease risk, hidden familial relationships, and other phenotypic information such as emotional stability, mental capacity, appearance, and physical abilities. Obtaining meaningful, informed donor consent and ensuring genomic data processing remains in sync with

[10] Examples of the types of problems individuals may experience as a result of genomic data processing activities include dignity loss, discrimination, loss of autonomy, and loss of trust. See Sec. 2.3 of this Profile for further discussion regarding the relationship between cybersecurity and privacy risk.

their consent over time provides some control to individuals to address concerns they might have about data sharing and aggregation. For these reasons, managing consent is an important area of focus for organizations, especially if genomic data is shared or aggregated. Additionally, donor consent may not adequately consider potential impacts on relatives.

- **Discrimination concerns** can also stem from sample bias. Artificial intelligence and statistical techniques analyze large sets of genomic data to predict disease and treatment efficacy. Predominantly, these analyses currently use data sets where minority communities are underrepresented. Lack of sample diversity can impact the results and cause discrimination with corresponding potential harms to those not well represented in the sample set [12][13][14].
- **National security concerns** arise from genomic data's ability to uniquely identify individuals, their kinship to others, phenotypes, and mental and physical health risks. Concerns include genomic data's use for population surveillance or extortion of citizens, military and intelligence personnel, and in other circumstances where genomic information reveals vulnerabilities in specific, high-profile individuals or persons of interest [15].

This Profile is designed to help organizations address the cybersecurity and privacy aspects of these concerns by identifying, prioritizing, and achieving the outcomes that are appropriate for their Mission Objectives and the sensitivity of the genomic data they are processing.

3. The NIST Cybersecurity and Privacy Frameworks

Created through collaboration between industry and government, the NIST CSF and PF provide prioritized, flexible, risk-based guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, reduce, and communicate cybersecurity and privacy risks. The background provided in this section is provided to make this document self-contained for all audiences, but may be skimmed by those with more familiarity with the CSF and PF.

The CSF and PF enable organizations—regardless of size, degree of cybersecurity and privacy risk, or cybersecurity and privacy sophistication—to apply the principles and recommended practices of risk management to improve security and resilience. The two frameworks provide a common language for understanding, managing, and expressing cybersecurity and privacy risk and for conducting management-level cybersecurity and privacy communications among internal and external stakeholders and across an organization, regardless of cybersecurity or privacy expertise.

The CSF and PF each consist of three main components[11]:

1. The **Core** is a taxonomy of desired cybersecurity or privacy activities and outcomes using common language that is easy to understand regardless of cybersecurity or privacy expertise. The Core guides organizations in managing and reducing their cybersecurity and privacy risks to complement an organization's existing cybersecurity and privacy risk management processes.

2. **Tiers** characterize the rigor of an organization's cybersecurity and privacy risk governance and management practices, and they provide context for how an organization views cybersecurity or privacy risk management. Tiers help set the overall tone for how an organization will manage its cybersecurity and privacy risks and understand the extent to which this risk management integrates with broader organizational risk management decisions. (Although part of the CSF and PF, for the purposes of this Profile, further discussion on Implementation Tiers is excluded.)

3. **Profiles** are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes for organizations and communities. Profiles provide a customized alignment of requirements, objectives, risk appetite, and resources against the desired outcomes of the CSF or PF Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity or privacy in a specific context (e.g., an organization's mission needs or a community use case like processing genomic data).

[11] The terms Core, Tiers, Profile, Mission Objectives, Function, Category, and Subcategory are capitalized when they are used to describe elements of the CSF throughout this document.

3.1. The Core

The CSF or PF Core articulates activities and outcomes using common language that all levels of an organization, from the executive level to the individuals with operational roles, can understand. It also provides examples of available resources to help organizations achieve those outcomes. At the top level, the Framework Cores are organized by concurrent and continuous Functions. When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of privacy and cybersecurity risk. The Functions are further subdivided into Categories and Subcategories to convey outcomes for each Function. Table 1 (Sec. 3.1.1) and Table 2 (Sec. 3.1.2) present the Functions and Categories in the CSF and PF.

The Core in each Framework is also supported by Informative References, which are mappings that indicate relationships between the Core and various standards, guidelines, regulations, and other content to help inform organizations on achieving those outcomes. Communities and organizations can choose to add additional Informative References unique to the genomic data processing context in the future. Sections 3.1.1 and 3.1.2 further describe the CSF and PF Cores.

NIST also provides supplemental resources to help organizations understand, adopt, and use the CSF 2.0, including Implementation Examples. These resources provide practical guidance to help an organization achieve the desired outcome of each Subcategory. The NIST CSF and PF websites (Appendix A) contain the most current information regarding available Informative References.

3.1.1. The Cybersecurity Framework Core

The CSF 2.0 Core consists of six concurrent and continuous Functions: Govern, Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

- **Govern (GV)**: *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The Govern Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. Govern addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
- **Identify (ID):** *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under Govern. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures,

and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **Protect (PR):** *Safeguards to manage the organization's cybersecurity risks are used.* Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

- **Detect (DE):** *Possible cybersecurity attacks and compromises are found and analyzed.* Detect enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

- **Respond (RS):** *Actions regarding a detected cybersecurity incident are taken.* Respond supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored. Recover supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

The CSF 2.0 Core identifies underlying Categories and Subcategories for each Function. Table 1 presents the six Functions including 22 Categories of cybersecurity outcomes such as "Organizational Context" and "Platform Security."

Table 1. Cybersecurity Framework Functions and Categories.

Category Unique Identifier	CSF FUNCTION: Category Title
GV.OC	GOVERN: Organizational Context
GV.RM	GOVERN: Risk Management Strategy
GV.RR	GOVERN: Roles, Responsibilities, and Authorities
GV.PO	GOVERN: Policy
GV.OV	GOVERN: Oversight
GV.SC	GOVERN: Cybersecurity Supply Chain Risk Management
ID.AM	IDENTIFY: Asset Management
ID.RA	IDENTIFY: Risk Assessment
ID.IM	IDENTIFY: Improvement
PR.AA	PROTECT: Identity Management, Authentication, and Access Control
PR.AT	PROTECT: Awareness and Training

Category Unique Identifier	CSF FUNCTION: Category Title
PR.DS	PROTECT: Data Security
PR.PS	PROTECT: Platform Security
PR.IR	PROTECT: Technology Infrastructure Resilience
DE.CM	DETECT: Continuous Monitoring
DE.AE	DETECT: Adverse Event Analysis
RS.MA	RESPOND: Incident Management
RS.AN	RESPOND: Incident Analysis
RS.CO	RESPOND: Incident Response Reporting and Communication
RS.MI	RESPOND: Incident Mitigation
RC.RP	RECOVER: Incident Recovery Plan Execution
RC.CO	RECOVER: Incident Recovery Communication

The Categories are further broken down into 106 Subcategories of specific technical or management activities. Sec. 6 presents the prioritization for all 106 Subcategories for each Mission Objective, using one table for each of the 22 Categories in the CSF Profile.

3.1.2. The Privacy Framework Core

The PF 1.0 Core consists of five Functions: Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. The -P suffix is used in every Function, Category, and Subcategory to clearly indicate that it belongs to the PF.

- **Identify-P**: Develop the organizational understanding of how to manage privacy risks for individuals arising from data processing. The activities in the Identify-P Function are foundational for privacy risk management by establishing an understanding of inventory and mapping, the business environment, assessing risk, and managing privacy risks in the data processing ecosystem.
- **Govern-P**: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization’s risk management priorities that are informed by privacy risk. The activities in the Govern-P Function focus on organization-level activities such as establishing organizational privacy values and policies and identifying legal and regulatory requirements that enable an organization to prioritize its efforts consistent with its risk management strategy and business needs.
- **Control-P**: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. The activities in the Control-P Function consider data processing management from the standpoint of both organizations and individuals.
- **Communicate-P**: Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks. The activities in the Communicate-P

Function address how organizations and individuals communicate and understand how data are processed to manage privacy.

- **Protect-P**: Develop and implement appropriate data processing safeguards. The activities in the Protect-P Function cover data protection to prevent cybersecurity-related privacy events and represent the overlap between privacy and cybersecurity risk management.

Table 2 shows the Core elements of PF 1.0, including 18 Categories. The PF Categories are further divided into 100 PF Subcategories.

Table 2. Privacy Framework v1.0 Core Functions and Categories.

Category Unique Identifier	PF FUNCTION: Category Title
ID.IM-P	IDENTIFY-P: Inventory and Mapping
ID.BE-P	IDENTIFY-P: Business and Environment
ID.RA-P	IDENTIFY-P: Risk Assessment
ID.DE-P	IDENTIFY-P: Data Processing Ecosystem Risk Management
GV.PO-P	GOVERN-P: Governance, Policies, Processes, and Procedures
GV.RM-P	GOVERN-P: Risk Management Strategy
GV.AT-P	GOVERN-P: Awareness and Training
GV.MT-P	GOVERN-P: Monitoring and Review
CT.PO-P	CONTROL-P: Data Processing, Policies, and Procedures
CT.DM-P	CONTROL-P: Data Processing Management
CT.DP-P	CONTROL-P: Disassociated Processing
CM.PO-P	COMMUNICATE-P: Communication Policies, Processes, and Procedures
CM.AW-P	COMMUNICATE-P: Data Processing Awareness
PR.PO-P	PROTECT-P: Data Protection Policies, Processes, and Procedures
PR.AC-P	PROTECT-P: Identity Management, Authentication, and Access Control
PR.DS-P	PROTECT-P: Data Security
PR.MA-P	PROTECT-P: Maintenance
PR.PT-P	PROTECT-P: Protective Technology

3.2. Community Profiles

A Community Profile describes CSF or PF outcomes to address shared interests and goals for reducing cybersecurity or privacy risk among multiple organizations that share a common context, such as sectors or technologies. Community Profiles offer a prioritization of CSF and PF Subcategories based on priority mission and operational considerations for a specific community, industry, or group of stakeholders, such as the genomics community. Community Profiles can also inform development of an organization’s Target Profile by providing a useful starting point for identifying and engaging in discussions about cybersecurity and privacy activities and outcomes important to the Profile’s user community. Within an organization, Target Profiles offer a consistent way to discuss cybersecurity and privacy objectives across organizational roles—from senior leadership to technical implementors—using common terminology.

This Profile is oriented around Mission Objectives, though some Profiles take a different approach. Mission Objectives are high-level goals that organizations in the genomics community strive to achieve to succeed in meeting their primary mission. Those in this Profile provide the context for managing cybersecurity and privacy risk as it relates to a specific mission need. This Profile prioritizes the Subcategories that are especially relevant to each Mission Objective. An organization can adapt Mission Objectives and Subcategory prioritization to fit its unique needs. Community Profiles can help organizations allocate resources to cybersecurity and privacy improvements or to address areas of specific risk.

3.3. Applying the NIST Frameworks to Genomic Data

This Genomic Data Profile prioritizes CSF and PF Core Subcategories designed to help an organization protect genomic data throughout the data life cycle (illustrated in Fig. 1). Organizations can use the Profile guidance, rationale, and considerations to examine and potentially improve their existing cybersecurity and privacy practices and activities. Organizations that process human genomic data can use the prioritized PF Subcategories to address privacy concerns more fully, such as managing donor consent preferences throughout data processing.

Organizations may apply the Genomic Data Profile to their organization by first identifying and describing their mission and business objectives. Sec. 5 details 12 Mission Objectives for the genomic data ecosystem developed with stakeholder input. Organizations may apply these or similar Mission Objectives or develop their own. Each organization can prioritize Mission Objectives based on their requirements and strategic goals.

Next, organizations can crosswalk their Mission Objectives to the Genomic Data Profile's Subcategories, using the tables in Sec. 6 to identify priority Subcategories. They can use the General Rationales and Mission Objective Specific Considerations from Sec. 6 to adjust the priority of Subcategories to reflect their organizational needs. During this activity, organizations consider any constraints or guidance (e.g., applicable state laws, policies, standards), risks, and other influencing factors that can impact their Mission Objectives or the priority of Subcategories. At each step, organizations can document rationales, considerations, and any additional Informative References. This results in an Organizational Target Profile.

Based on their review and adjustment of Mission Objectives and priority Subcategories, organizations examine their current cybersecurity and privacy activities and processes to create an Organizational Current Profile. Organizations can then identify any gaps between their Current and Target Profiles. This gap analysis can help an organization determine if they need to reallocate cybersecurity and privacy resources toward capabilities that help achieve prioritized Subcategories and accomplish the organization's Mission Objectives. Additionally, organizations can compare their Current Profile to the Genomic Data Profile to see how their activities compare to the genomics community's priorities.

4. Genomic Data Profile Development Methodology

Developing a Community Profile is a collaborative stakeholder-driven process. Stakeholders who are experts across the genomics community contributed to this Profile to ensure that it aligns cybersecurity and privacy outcomes with business and mission requirements. This section describes how the NCCoE gathered input and garnered consensus from a diverse group of stakeholders to produce this Profile.

From October 2022 through February 2023, the NCCoE hosted virtual working sessions with genomics community stakeholders from government, academia, a nonprofit think tank, and industry, including instrument manufacturers and cloud service providers. The working sessions sought to develop and prioritize Mission Objectives for the Genomic Data Profile and to prioritize CSF 1.1 Categories for each Mission Objective (this work was completed before CSF 2.0 was released). The NCCoE solicited input from the stakeholders, who served as subject matter experts (SMEs), to identify objectives specific to managing and maintaining genomic data ecosystems at their organization and in the genomic data ecosystem. Following the completion of the stakeholder working sessions, the NCCoE team of genomic data and cybersecurity SMEs analyzed the outputs from the stakeholder Category prioritization and used them to inform CSF Subcategory priorities for each Mission Objective. During Subcategory discussions, the NCCoE team documented general rationales for why an organization would prioritize a Subcategory along with specific rationale for prioritizing Subcategories for each Mission Objective. This process resulted in the draft CSF Profile for Genomic Data, which was released for public comment in June 2023.

From September through November 2023, the NCCoE held additional working sessions to identify privacy priorities. During the privacy sessions, the team reviewed and validated the Mission Objectives to verify that they appropriately reflected the priorities of the genomic community. The resulting 12 prioritized Mission Objectives are described in Sec. 5 of this Profile. Then the team of privacy and genomic SMEs collaborated to prioritize PF Categories. The team followed the same process described for the CSF for the PF.

In February 2024, NIST published CSF 2.0. The NCCoE used the previous inputs from the CSF 1.1 discussions and a crosswalk of CSF 1.1 to CSF 2.0 to analyze and recommend CSF 2.0 priority Subcategories for the Genomic Data Profile. Consistent with the methodology related to maintaining a Profile, the NCCoE team also analyzed previously prioritized Subcategories to determine if adjustments were needed (i.e., priorities, rationale statements) based on new or additional information (e.g., genomic data processing environments, safeguards in place or gaps, potential threats) that could impact the information in this Profile.

The details from these analyses are summarized in Sec. 6 of this document, serving as the primary content in this Genomic Data Profile. In January 2024, NIST announced it would be updating the PF, which would influence the future direction of the Genomic Data Profile.

5. Genomic Data Mission Objectives

The working session discussions resulted in 12 Mission Objectives that characterize high-level critical operational needs for an organization to meet its primary mission in the genomic data processing ecosystem. The Mission Objectives are operational imperatives. In some cases, the Mission Objectives are focused on cybersecurity or privacy needs, though the overall set of objectives are broader than cybersecurity or privacy. Although the Mission Objectives are discussed as discrete ideas, there are interdependencies between many of them.

During the working sessions, stakeholders ranked the Mission Objectives based on priority levels shown in Table 3. Their prioritization is meant to be informative rather than prescriptive. Interdependencies between Mission Objectives played a role in the prioritization. In some cases, interdependencies elevated the prioritization of an individual Mission Objective (e.g., Data Quality has such a strong relationship to most of the other Mission Objectives and was prioritized first). In other cases, certain aspects of related Mission Objectives rated higher than others (e.g., managing privacy risks to individuals was divided between donors and relatives; even though the two are related concepts, with relatives having a dependency on donors, the unique needs for relatives led to higher prioritization of managing privacy risk to relatives than donors). Each organization can consider its own goals and priorities when consulting this Profile and adjust how it applies the guidance accordingly. For example, when using this Profile to create an Organizational Target Profile, organizations may add or remove a Mission Objective, re-prioritize Mission Objectives, edit phrasing or terminology, or combine or deconstruct a Mission Objective to more closely align with their own needs.

An example of using these Mission Objectives follows: ABC Co. ("ABC") is a small new genomic research company that processes human genomic data and has a low cybersecurity and privacy maturity. Using Table 3, ABC can select the most important Mission Objectives (MOs) that apply to their organization and determine the most important CSF and PF Subcategories that the organization can use to prioritize its cybersecurity and privacy programs. For example, ABC can select MOs 1 (data), 2 (relatives), 5 (donors), and 8 (research). While implementing their Organization Target Profile, they can prioritize these MOs and then start by addressing those Subcategories identified as High Priority.

Table 3. Genomic Data Profile Mission Objectives.

Priority	Genomic Data Profile Mission Objective (Keyword)
1	Manage provenance and data quality throughout the genomic data life cycle (Data)
2	Manage privacy risk to existing and future relatives (Relatives)
3	Identify, model, and address cybersecurity and privacy risks of processing genomic data (Risks)
4	Manage informed consent throughout the genomic data life cycle (Consent)
5	Manage privacy risk to donors (Donors)
6	Manage authorized data access (Access)
7	Maintain trustworthiness and manage reputational risk (Trust)
8	Facilitate research and education to advance science and technology (Research)
9	Maintain compliance with laws and regulations (Legal)
10	Protect intellectual property (IP)
11	Ensure the degree of diversity is appropriate for processing purposes (Diversity)
12	Promote the use of privacy-enhancing technologies as well as secure technologies for sharing genomic data (Tech)
ALL	*These Mission Objectives apply to the integrated Genomic Data Profile.*
CSF	*The CSF addresses cybersecurity aspects of these Mission Objectives.*
PF	*The PF addresses the privacy aspects of these same Mission Objectives.*

Descriptions for each Mission Objective follow, including a rationale for the prioritization of the Mission Objective and a keyword used to identify the Mission Objective in the tables in Priority Subcategories by Mission Objective.

5.1. Objective 1: Manage provenance and data quality throughout the genomic data life cycle (Data)

Provenance provides a chronology of what happens to genomic data from its origin through processing, including documenting originating sources, sequence data, changes in custody, annotations, derived data, data version, software version, software configurations, and analysis parameters. Tracking provenance throughout the data life cycle, especially as data changes hands, helps organizations process data that are valid and appropriate. Provenance in the genomic data life cycle can be maintained when introducing any data series.

Data quality practices ensure genomic data are sufficiently timely, relevant, accurate, and complete for processing purposes. In this context, data quality also encompasses standard quality control metrics and experimental design considerations and extends to ensuring that data are appropriate for their intended purpose and potentially suited for additional processing activities (for example, for further analyses). The complex genomic data life cycle introduces challenges in maintaining the data provenance and authenticity required for use by the genomics community. Effectively managing the genomic data life cycle supports data provenance and quality, which support cybersecurity and privacy risk management.

Data quality protections can include assurances that data are appropriate for processing purposes and will provide valid analyses and results, and that the chain of provenance remains intact. The data are protected to maintain quality throughout the data life cycle using hardware and software controls as well as effective data storage and analysis. Data quality also includes the secure dissemination and sharing of data sets through properly protected interconnected systems.

Sharing genomic data is uniquely relevant to this process because it becomes increasingly difficult to preserve original source rights and privacy rights over time as data are shared with and processed by other organizations. Integrating data quality assurances at the start of the data life cycle, such as during research study design, also improves cybersecurity and privacy outcomes. Accurate and scalable data inventories and data flows can help identify potential data sources and endpoints, support risk assessments, and protect data quality throughout the genomic data life cycle.

Rationale: Data provenance and quality were identified as the highest priority because of their impact on all Mission Objectives. If the data cannot be trusted, then the research, investigations, and consumer services will be inherently flawed.

5.2. Objective 2: Manage privacy risk to existing and future relatives (Relatives)

The commonality of genomic data among deceased, living, and future biological relatives can reveal health conditions, disease histories, and unknown relations. It can also facilitate discrimination, as well as physical and financial harm towards identifiable populations. The sensitivity of information that can be revealed regarding donor relatives warrants careful management and control of genomic data. Organizations can identify where privacy risks to relatives might arise due to an organization’s role in the genomic data processing ecosystem and in their internal operations. Information about relatives can be safeguarded from potential privacy harms such as genetic association (for example, social, economic, and psychological) or the non-consensual usage of their genomic information. These harms to relatives are considered throughout the data processing life cycle. For example, determining the impact of combining data sources, such as re-identification, can inform data-sharing practices. Risk and harm can also inform retention policies and other processes for protecting the privacy of relatives.

Rationale: Relatives’ privacy was rated highly because of the number of people impacted and the fact that relatives are not directly involved in the data collection process. Relatives may not be aware of a donor's actions and the impact of donor decisions on them. Relatives also do not have the opportunity to provide consent for the use of or inferences that may come from the donor’s genomic data. This Mission Objective highlights the importance of managing access to information pertinent to living and future relatives to protect the privacy rights of all familial matching individuals (i.e., people in a genetic family). Some aspects of privacy rely on cybersecurity, such as controlling access to information about relatives that may be included when processing genomic data. The stakeholders highlighted the privacy impact on relatives because it can potentially be overlooked and advances in technology may introduce unanticipated privacy impacts.

5.3. Objective 3: Identify, model, and address cybersecurity and privacy risks of processing genomic data (Risks)

Genomic information is subject to a variety of evolving security threats, from hardware and software vulnerabilities to the misuse of information, and privacy problems, such as dignity loss, discrimination, or loss of autonomy because of unanticipated revelation of health conditions or progeny. Addressing risks of processing genomic data protects bioeconomy interests from adverse outcomes to individuals and populations, such as discrimination, exploitation, or abuse, and to organizations, such as reputation or financial. The genomics community can address known cybersecurity threats and privacy problems associated with processing genomic data by using risk management tools, such as cybersecurity and privacy standards and threat modeling. Improved understanding of risk can help organizations select appropriate practices and review and update those practices to ensure they address emerging capabilities that introduce new risks, such as quantum computing.

Rationale: This Mission Objective was rated highly because business operations may be disrupted or impaired due to ineffective cybersecurity or privacy capabilities. Also, this Mission Objective may highlight business processes that could introduce unique risks to an organization. Cybersecurity and privacy risks may result in ransomware, data exfiltration, data quality issues, and donors or partners deciding to no longer participate with the organization.

5.4. Objective 4: Manage informed consent throughout the genomic data life cycle (Consent)

Organizations institute policies and practices for providing meaningful notices and obtaining and maintaining informed consent prior to collecting or processing human donor information. They also ensure that consent requirements travel with genomic data when it is shared. At a minimum, consent includes providing these donors information about the organization’s data processing practices (sometimes referred to as a privacy notice), including operational activities and privacy and security protections, donor rights, and privacy points of contact in a way that clarifies the terms of consent.

Organizations can ensure that their operational practices, equipment, and technologies conform to the agreements they make with donors through the consent process. Procedures to review consent as needed are established to ensure that the operational environment and donor consent remain in sync over time, such as when technologies enable new processing capabilities or when genomic data is shared with new partners. Special care needs to be taken regarding the use of secondary data subjects (relatives), who often do not have mechanisms to participate in donor notice and consent processes. Organizations can consider how to ensure that notice and consent are meaningful for all parties and implement measures to protect secondary data subjects.

Rationale: While much of consent relies on privacy processes, cybersecurity plays a role in ensuring data processing activities are consistent with consent through appropriate access controls and data protection mechanisms. Donors may be hesitant to share their genomic data without adequate transparency and commitment from the organization to manage their genomic data in accordance with a clear statement of benefit for the donor’s participation. The consent statement clearly describes the permitted processing of their donated data and includes an unambiguous request for revokable consent in alignment with this statement. Prioritization of this Mission Objective is impacted by the fact that it applies only to human genomic data.

5.5. Objective 5: Manage privacy risk to donors (Donors)

Processing human genomic data presents some unique privacy challenges. Privacy risks can occur throughout the data processing life cycle. For example, determining the impact of combining data sources, such as re-identification, can inform data-sharing practices. Risk and harm can also inform retention policies and other processes for protecting the privacy of donors. Organizations can review these recommendations and consider applying this guidance in the context of their role in the genomic ecosystem, taking into consideration both the needs and expectations of genetic donors and their relatives, as well as the safeguards and limitations of individual informed consent. In addition, appropriate cybersecurity safeguards help protect against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of genomic data.

Rationale: Donors will be hesitant to provide their genomic data unless they trust that organizations will follow appropriate privacy practices. Some aspects of privacy rely on cybersecurity, such as protecting information about donors when processing genomic data. By managing risk to the donor’s privacy, organizations maintain the donor’s trust and are better able to comply with local, national, and international laws and regulations. Measures that protect the donor’s information can also manage some privacy risks to relatives (Mission Objective 2). Prioritization of this Mission Objective is impacted by the fact that it applies only to human genomic data.

5.6. Objective 6: Manage authorized data access (Access)

Without certain precautions, genomic data can be accessed and exploited by unauthorized users. Organizations can establish data access controls that manage appropriate access to genomic data and prevent unauthorized usage. Establishing controls with appropriate levels of access enables authorized usage, providing information containment without impacting necessary activities such as data analysis. Data access can be granted solely from a managed authority. These controls manage who can access data, who has authority to grant access, and what permissions can be granted. These permissions can be modified or revoked in alignment with the terms of consent and use. Processes to manage access authorities in accordance with changes to consent both prevent unauthorized access and manage authorized access.

Rationale: While managing access to data can be viewed as a risk management activity under Mission Objective 3, it was identified as a distinct area of focus given the heavy reliance on access management for both cybersecurity and privacy. Granting access to authorized users and preventing unauthorized usage enables other Mission Objectives. Organizations put measures in place to monitor access and ensure appropriate personnel are accountable for managing the risk that may arise from data access.

5.7. Objective 7: Maintain trustworthiness and manage reputational risk (Trust)

Organizations institute practices that meet the needs of stakeholders to form the foundations that establish and maintain trust. Trustworthiness is a necessary foundation that affects whether and how stakeholders participate in the genomic data ecosystem. This trust relationship helps donors have confidence contributing to genomic data activities and ensures that the public may continue deriving value from those activities. Trust also impacts an organization's ability to collaborate effectively with other organizations throughout the genomics community. It is vital that trust-building activities be tailored to reflect the needs of different subgroups described by social, biological, geographic, or other factors, and to address privacy problems. Organizations can build and maintain trust through responsible and effective genomic data management, privacy, and security practices, including building trustworthy systems, along with the legal and regulatory compliance described in other Mission Objectives. Additionally, organizations manage reputational risk to maintain credibility and a positive public perception.

Rationale: Individuals need to trust organizations before they will participate in genomic data activities. Failure to maintain trustworthiness and manage reputational risk could put other Mission Objectives at risk when organizations or individuals decide not to collaborate or work with an organization.

5.8. Objective 8: Facilitate research and education to advance science and technology (Research)

Investments in genomic research and education that will train the next generation of geneticists and biologists can help unlock new scientific and technological breakthroughs. Ways to facilitate genomic research and education include providing hands-on guidance and best practices; supporting collaborative genetic research; and supporting the safe use of genetic information to improve the health of our populations and environment [e.g., the U.S. Centers for Disease Control and Prevention's (CDC) One Health initiative[12]]. Ensuring clear communication and understanding between scientific and cybersecurity professionals for safe storage and management of genomic data can prevent potential data loss and disruptions to research. Maintaining the integrity and availability of the research environment can also help ensure the reproducibility of a study.

Rationale: Organizations focused on research and education prioritized this Mission Objective higher than others. Research and education enable the full potential and usage of genomic data. This Mission Objective overlaps with other Mission Objectives (1, 3, 6, 12) that support authorized data sharing, data quality, and comprehensive data sets. New technologies (Mission Objective 12) may benefit researchers but also may introduce complexities for evaluating and maintaining compliance.

[12] More information about CDC's One Health initiative can be found at https://www.cdc.gov/onehealth/index.html.

5.9. Objective 9: Maintain compliance with laws and regulations (Legal)

Organizations processing genomic data are required to comply with applicable laws and regulations. Organizations can make risk-based determinations regarding which countries to maintain operations in that best align their business priorities with the constraints of applicable laws and regulations. Organizations can ensure their activities support Good Practices (GxP) and other standards of practice. International data sovereignty and privacy rights may impose unique challenges that require stricter compliance with laws and regulations.

Rationale: Compliance with laws and regulations represents the foundation for processing and protecting genomic data and is part of fostering a responsible and trustworthy genomic data processing environment. While complying with laws and regulations is mandatory to conduct business and manage reputational risk, compliance is not typically a primary operational objective. Rather, compliance is a part of conducting business. It was ranked lower due to the increased focus on Mission Objectives that address issues beyond compliance, including managing where data is processed and how it is shared in conjunction with Mission Objectives 1 and 8.

5.10. Objective 10: Protect intellectual property (IP)

Safeguarding IP is a core function of many organizations. Organizations working with genomic data and developing IP, such as trade secrets or patentable information, protect these assets and associated business interests. Although withholding the release of genomic data may provide a competitive advantage to the holder, it could be detrimental to the genomics community. Still, some organizational operations require sequestering genomic information and associated analyses until they can be responsibly shared or disclosed. In addition, securing IP can also help establish and/or trace data ownership and provenance once the data is released externally.

Rationale: This Mission Objective broadly represents an inherent component of business operations. Organizations will continue to own and protect their inventions and investments, and the priority of this Mission Objective will reflect each organization’s specific requirements for their own IP.

5.11. Objective 11: Ensure the degree of diversity is appropriate for processing purposes (Diversity)

Establishing an appropriate degree of diversity in genomic datasets helps close disparities by ensuring that all populations benefit from health discoveries. Diversity needs vary based on the context of processing and may require coordination with multiple organizations to ensure that populations are well-represented while preventing unwanted identifiability of individuals, especially those in vulnerable sub-populations. Genomic sample diversity enables researchers to identify genetic variants with greater statistical confidence, allows for a more comprehensive and inclusive understanding of diverse populations, improves research and health outcomes, and potentially reduces privacy risk.

Rationale: In some contexts, human genomic data sets lacking representation from certain populations can skew results or potentially introduce privacy concerns when few individuals from an under-represented or vulnerable subgroup are included in the dataset. This Mission Objective rated lower because the activities required to conduct this Mission Objective may involve processes that happen prior to the genomic data collection. Additionally, this Mission Objective applies to all other Mission Objectives processing human genomic data.

5.12. Objective 12: Promote the use of privacy-enhancing technologies (PETs) as well as secure technologies for sharing genomic data (Tech)

Many organizations prefer to keep their data in one place they control rather than duplicating it across multiple internal and external environments. Privacy-enhancing technologies (PETs) can facilitate uploading, analysis, and collaboration, and help control downloading genomic data. The benefits of this approach include the ability to enforce consistent security practices that manage provenance, ensure data quality, restrict access to authorized entities, and enhance incident/breach response while enabling safe and controlled use of the genomic data. Organizations can also support the implementation of emerging technologies and international standards for the transfer of clinical and administrative data between software applications used by various healthcare providers.

Rationale: This Mission Objective reflects the rapid innovation in the genomic community and the value of promoting effective ways of sharing genomic data. As PETs and other technologies are developed and additional use cases are identified, organizations can make risk-based decisions to employ these in genomic workflows. This Mission Objective applies to the use and implementation of new technologies to be used along with other effective mechanisms for data access and confinement.

6. Priority Subcategories by Mission Objective

Following the methodology outlined in Sec. 4, NCCoE working sessions led the stakeholders through a process to score what they considered the most important CSF and PF Categories for implementing each Mission Objective. This section presents the results of analyzing the stakeholders' Category prioritization and related discussions to prioritize the selection of the 106 CSF Subcategories and 100 PF Subcategories for each Mission Objective.

Each Subcategory was assigned High, Moderate, or Other priority, along with a rationale to help explain the relative importance of a Subcategory to a Mission Objective.

The Subcategories' priority importance is indicated in each Table:

- One (**"1"**) for High Priority: These represent the most critical Subcategories for enabling a Mission Objective that are typically addressed most immediately, given available resources.
- Two ("2") for Moderate Priority: These Subcategories are typically the next priority after implementing High Priority Subcategories and may become higher priority in certain contexts or environments to implement a given Mission Objective.
- Three ("3") for Other Priority: These Subcategories are important to the overall cybersecurity and privacy aspects of a Mission Objective but may not require the same level of urgency as higher priority Subcategories. Note that "Other Priority" does not equate to low priority. All Subcategories should receive consideration.

Following the guidance in Sec. 3.3, organizations can use the tables below to prioritize cybersecurity and privacy Subcategories that align with their Mission Objectives. Although organizations should develop strategies that address all Subcategories, the prioritization provides adaptable guidance that suggests cybersecurity and privacy capabilities that will provide the greatest impact toward meeting Mission Objectives for organizations in the genomics community.

- **CSF to PF Crosswalk**
  Table 4 through Table 25 presents the detailed results of this Subcategory analysis, presented for each CSF Category. Each table includes all the CSF Subcategories for a single CSF Category, along with the PF Subcategories that are cross-walked to that CSF Subcategory.[13] The crosswalk provides an integrated approach to address related cybersecurity and privacy Subcategories together. Rows for each CSF Subcategory are indicated by the color code for that CSF Category across all Mission Objectives. Rows for PF Subcategories follow the related CSF Subcategory but are not colored. Rows for repeated PF Subcategories are included without the details for the Subcategory.
- **Unique PF Subcategories**
  Table 26 through Table 36 present the PF Subcategories that do not crosswalk to CSF 2.0

[13] NIST defined a DRAFT alignment that provides a crosswalk between the CSF 2.0 and PF **1**.0 Subcategories to help visualize the integration of cybersecurity and privacy that will be updated with PF 1.1. The full draft can be downloaded from https://www.nist.gov/document/csf-11-20-pf-10-crosswalkdraft.

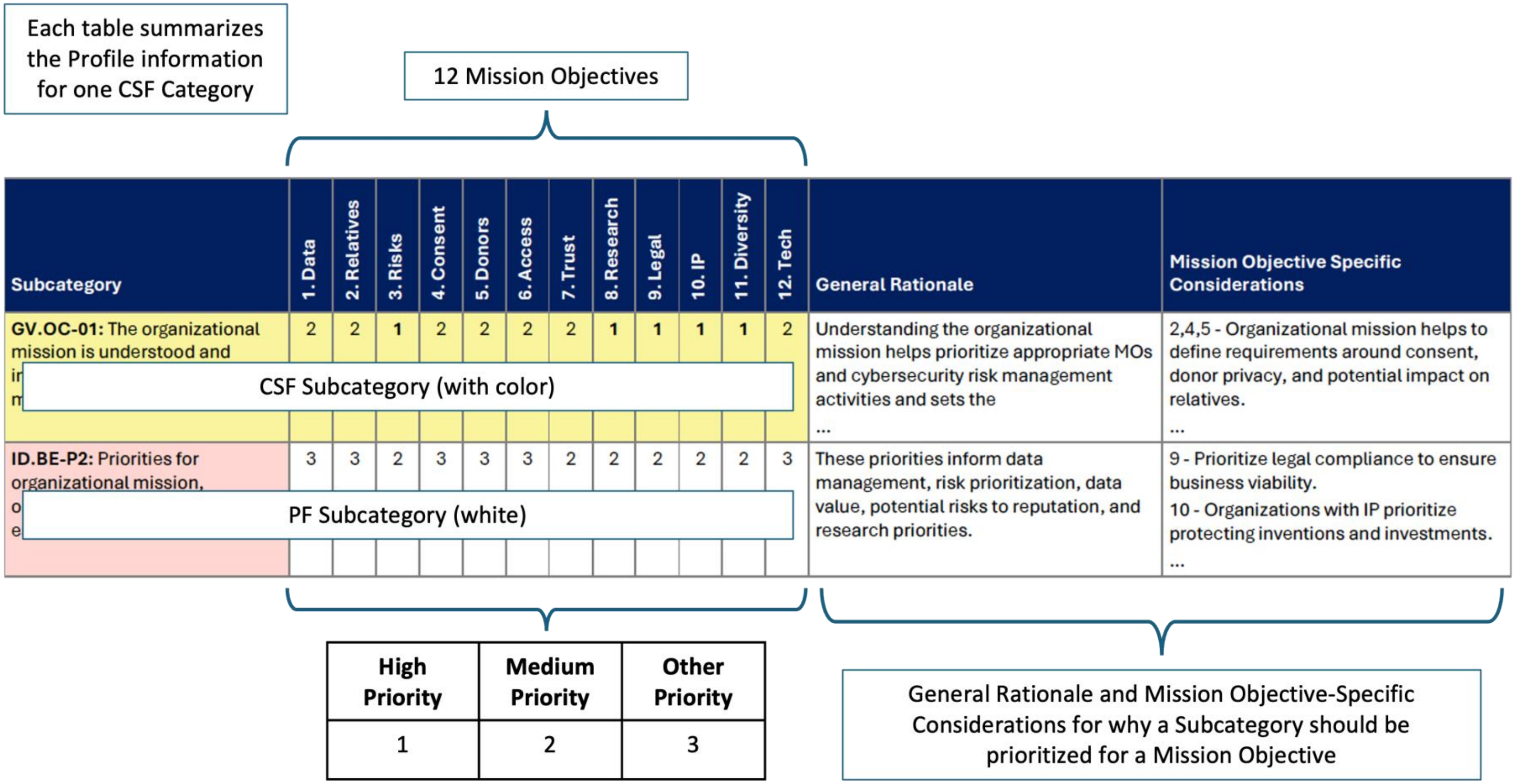
Subcategories, labeled as “Unique Privacy Framework Subcategories” with one table for each PF Category.

Note that the Tables could also be sorted by PF Category to include all PF Subcategories along with the CSF Subcategories that align with that PF Subcategory. However, this would result in twice as many Tables in this document. Each organization is invited to use the Genomic Data Profile Spreadsheet Tool[14] to customize the content of the tables and export the information as required.

As shown in Fig. 4, each of the CSF to PF Crosswalk tables starts with the description of the CSF Category. [Note: For the Unique PF Subcategories, the table description includes the PF Function and the PF Categories appear as a unique row in the table; otherwise the tables are similarly formatted.] The numbers 1 to 12, along with the keyword in the table, align with the 12 Mission Objectives from Table 3 (Sec. 5). Each table row identifies the CSF or PF Subcategory and the priority of that Subcategory for every Mission Objective using the numbers 1, 2, or 3.

Each table includes columns for General Rationale and Mission Objective Specific Considerations, indicating why the Subcategory would be prioritized for an organization. The General Rationale column provides organizations with Mission Objective-agnostic content that may inform an organization's prioritization of a Subcategory. The Mission Objective Specific Considerations column provides organizations with context specific to a given Mission Objective for why a Subcategory could be elevated in priority. The Tables use the acronym MO for Mission Objective for brevity.

[14] The Genomic Data Profile Spreadsheet Tool can be found at the NCCoE Genomic Data website https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data



Each table summarizes the Profile information for one CSF Category

12 Mission Objectives

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.OC-01: The organizational mission is understood and ir m	2	2	**1**	2	2	2	2	**1**	**1**	**1**	**1**	2	Understanding the organizational mission helps prioritize appropriate MOs and cybersecurity risk management activities and sets the ...	2,4,5 - Organizational mission helps to define requirements around consent, donor privacy, and potential impact on relatives. ...
ID.BE-P2: Priorities for organizational mission, o e	3	3	2	3	3	3	2	2	2	2	2	3	These priorities inform data management, risk prioritization, data value, potential risks to reputation, and research priorities.	9 - Prioritize legal compliance to ensure business viability. 10 - Organizations with IP prioritize protecting inventions and investments. ...

CSF Subcategory (with color)

PF Subcategory (white)

High Priority	Medium Priority	Other Priority
1	2	3

General Rationale and Mission Objective-Specific Considerations for why a Subcategory should be prioritized for a Mission Objective

Fig. 4 Sample CSF Category Table with Descriptions.

Table 4 presents the CSF and cross-walked PF Subcategories for the Organizational Context (GV.OC) Category. The CSF description for this Category is: The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood.

Table 4. Govern: Organizational Context (GV.OC).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.	2	2	**1**	2	2	2	2	**1**	**1**	**1**	**1**	2	Understanding the organizational mission helps prioritize appropriate MOs and cybersecurity risk management activities and sets the foundation for defining threats, vulnerabilities, probabilities, and impacts for determining cybersecurity risks. The organizational mission also helps define the relationship between cybersecurity and privacy risk management. This is the basis for identifying applicable laws and regulations for protecting data (HIPAA [16], FISMA [17], GDPR [18], etc.).	2,4,5 - Organizational mission helps to define requirements around consent, donor privacy, and potential impact on relatives. 6,8,12 - Mission informs cybersecurity risk management decisions related to the value of the data used, results from research activities, and the need for or use of new technologies, supporting an organization's ability to manage impact from adverse events (e.g., unauthorized access) that may affect the mission. 9 - Legal and regulatory compliance enable the organization to achieve its mission. 10,11 - Priorities for protecting IP or ensuring sample diversity in support of the mission are understood.
ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	3	3	2	3	3	3	2	2	2	2	2	3	These priorities inform data management, risk prioritization, data value, potential risks to reputation, and research priorities.	9 - Prioritize legal compliance to ensure business viability. 10 - Organizations with IP prioritize protecting inventions and investments. 11 - Diversity needs vary based on the context of processing and may require coordination with multiple organizations.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														Clearly communicate priorities related to diversity to influence operations. 12 - Priorities determine how forward-leaning the organization is when embracing privacy-enhancing and secure technologies; ID.BE-P1 and -P3 more directly influence technology decisions.
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**1**	**1**	**1**	2	**1**	2	**1**	2	2	3	2	2	Organizations processing genomic data tend to share them with other data partners, resulting in a complex ecosystem required to produce the outcome. Defining the cybersecurity risks introduced by this diverse stakeholder-rich ecosystem helps manage data quality and provenance, legal compliance, coordinating across researchers, and maintaining compliance with security and privacy requirements.	1 - Data quality and provenance require managing any risk introduced by suppliers or partners. 2,4,5,8 - Each stakeholder in a genomic data processing relationship understands the relationship between cybersecurity and privacy risk management and expectations for how cybersecurity activities support privacy needs. For example, they understand their responsibilities to protect genomic data according to consent agreements and consider when additional access controls may be necessary to protect more sensitive data. Stakeholders are also aware of where additional measures are necessary to address the full scope of privacy risk by integrating Privacy Framework Subcategories. 11 - Partners sharing data consider cybersecurity requirements to ensure that all stakeholders protect and maintain sample diversity.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, and application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	**1**	2	**1**	3	**1**	2	2	2	2	3	2	2	This ecosystem privacy risk assessment across parties will help identify issues with data quality, provenance, privacy/consent, access controls, protection of IP, and sample diversity, as well as legal/regulatory compliance.	2,5 - Identify where privacy risks to relatives and donors might arise in the genomic data processing ecosystem, including re-identification. 7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem. 12 - Technologies support effective, controlled sharing of genomic data.
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed.	**1**	**1**	**1**	**1**	**1**	2	**1**	**1**	**1**	2	2	**1**	Laws and regulations will be implemented through organizational policy, processes, and procedures and documented in contracts. Security and privacy requirements, including civil liberties, will be prioritized across all MOs to meet legal requirements. Failure to meet these requirements introduces compliance and reputational risks.	1,3,8 - Compliance with laws and regulations provides foundational measures that help ensure that risks to data are appropriately managed throughout the life cycle and with partners, using contracts to enforce requirements. Managing risks may require additional measures beyond the minimum requirements expressed in laws, regulations, and contracts. 2,4,5 - Failure to comply with cybersecurity or privacy laws and regulations could deter donors from participating.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														7 - Reputation and trust will be damaged if laws and regulations are not followed. 9 - Legal and regulatory requirements are prioritized and enforced through organizational policy, processes, procedures, and contracts. 11 - Organizations remain cognizant of evolving legislation related to sample diversity. In the absence of requirements, organizations and affected communities work together to determine needs for specific genomic data processing purposes. 12 - Any impact on legal and regulatory compliance will be assessed as part of the acquisition or use of new technologies.
GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	**1**	**1**	**1**	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	Privacy values and policies will be highly prioritized across organizational activities involving genomic data and are best established at the highest levels of governance so that appropriate prioritization and consistency are provided. Most MOs ranked this Subcategory high because of how privacy policies dictate expectations for managing data quality, provenance, donors'/relatives' privacy, consent, reputation, shared data	2,4,5 - Relatives' privacy can be neglected. High-level policies that influence downstream practices can dictate and enforce privacy protection requirements for donors and relatives, including consent. 3 - Organizational policies can collectively act to protect general bioeconomy interests from adverse outcomes that are identified through risk assessment. 7 - Governance will need to address issues that may not be fully defined in laws and regulations. 6,10,12 - Policies set the expectation for data access management, IP protections,

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													partner expectations, legal compliance, and data diversity.	and when and how technologies are used inside the organization.
GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	2	2	2	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	Legal requirements will dictate how organizations manage the privacy and provenance of genomic data in a research ecosystem. Implementing controls, tracking metrics, and monitoring contractual agreements will demonstrate compliance and establish a baseline of trust for partnership collaboration.	2 - In some situations where the absence of specific legal requirements for the processing of genomic data may lead to data aggregation and inference (e.g., relatedness), organization-specific policies may be required to address potential privacy harms across an ecosystem. 4 - Consent needs to travel with data, and where specific laws do not address this requirement, policies could be used and incorporated into contracts. 5,11,12 - Even within a certain geography, other specific requirements may be necessary based on use case (e.g., clinical care, disease testing), ethnicity (e.g., Native Nations), or other regulations (HIPAA, GINA [19]).
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	2	3	2	3	2	2	2	**1**	2	2	2	2	Understanding any critical dependencies of stakeholders will help organizations with high availability requirements as well as understanding how the loss of those services could impact stakeholders' research or productivity, or even jeopardize security or privacy.	1,3 - The data life cycle is dependent on data quality to support essential services. The impact of these dependencies will be incorporated into risk management. 8 - Genomic researchers depend on sharing between partners and will identify dependencies that may introduce risks. 11 - Partners who share data consider stakeholder dependencies that include protecting and maintaining sample diversity throughout the life cycle.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														12 - Whenever using new technologies or platforms, organizations will assess any dependencies that may impact the availability or delivery of services.
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	2	2	**1**	3	2	2	2	**1**	**1**	2	2	2	Understanding any organizational critical dependencies helps organizations with high availability requirements understand how the loss of those services could impact outcomes such as research, production, security, or privacy.	1,3 - The data life cycle depends on data quality to support essential services. The impact of those dependencies will be incorporated into risk management. 2,4,5 - Privacy outcomes that rely on cybersecurity capabilities are included in dependencies. 7 - Issues with delivering services may result in other organizations losing trust in your organization. 8 - Researchers may not be able to deliver results without the services or sources they depend on. 9 - Organizations assess their role in the delivery of critical services and how legal compliance may be impacted through a disruption of services. 12 - Organizations determine dependencies on new technologies and services that may impact availability or the ability to deliver their own services.
ID.BE-P1: The organization's role(s) in the data processing ecosystem are	2	2	2	2	2	2	2	**1**	2	2	**1**	2	Organizational role (research, government, business) impacts data management choices and understanding of the genomic life cycle, especially for cross-organizational partnerships. Role	2,4,5 - Organizational role can inform management of donor and relative privacy and consent requirements when sharing data.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
identified and communicated.													also impacts priorities, risk tolerance, access requirements, reputational risk, legal requirements, and the degree of data diversity required. Communication increases transparency, promotes consistency in data handling, and builds trust.	7 - Context for use, social norms, perceptions, and political issues factor into trust and managing reputation. 8 - Understanding role in the research community supports the sharing of data within the research community, ensuring consent travels with data, monitoring potential risks, and monitoring changes for how data can be used for research across multiple participants. 12 - Technologies prioritize safe and controlled use of genomic data, factoring in the risk profile of data usage and its role in the ecosystem.

Table 5 presents the CSF and cross-walked PF Subcategories for the Risk Management Strategy (GV.RM) Category. The CSF description for this Category is: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

Table 5. Govern: Risk Management Strategy (GV.RM).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders.	2	2	**1**	2	2	2	**1**	2	2	**1**	2	2	Risk management processes help integrate cybersecurity and privacy activities for each MO.	1,3,10 - Risk management processes are integrated into the data processing life cycle and systems development life cycle. 2,4,5 - Risk management objectives incorporate cybersecurity and privacy objectives and an understanding of how the objectives may impact each other. 7,9 - Processes for managing reputational risk and legal and regulatory requirements are included. 12 - Users of technologies and platforms integrate risk management across all technologies used.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	**1**	2	**1**	3	2	3	2	**1**	**1**	**1**	3	**1**	Organizations use risk management processes to identify threats, controls, priorities, and resources required for privacy. Genomic data processing and life cycle risk management processes require organization-wide planning and implementation to meet legal, regulatory, and contractual requirements. Organizations protecting IP will want to tailor their risk assessment processes to include appropriate protections.	1,12 - Rapid advances in genomic-related technologies and data processing techniques will necessitate ongoing risk assessments to maintain effective application of controls and ensure data quality. 3 - Once a risk assessment is conducted, an organization will need a long-term strategy to guide the implementation of protocols and policies that are aligned with its goals and the protections needed. 8 - Research inherently broadens the reach of data, so risk assessment needs to be thought of as ecosystem-wide rather than limited to one organization. 11 - Risk assessments can help identify issues with sample diversity.
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained.	**1**	2	**1**	2	2	2	**1**	3	**1**	2	2	2	Risk appetite and tolerance help define priorities and thresholds that require risk response activities. Integrating risk tolerance into risk management may help to integrate more granular protections for genomic data.	1,6,7,10 - Risk tolerance helps define requirements and priorities for provenance, data quality, who can access the data, and what might cause reputational harm. 2,4,5 - Privacy requirements help define risk tolerances. 3 - Risk tolerance informs risk decisions and responses when a risk is realized. 9 - Laws and regulations help define organizational risk tolerance or thresholds.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	2	2	**1**	3	2	3	3	2	2	2	3	3	Risk tolerance guides organizational decisions on thresholds for privacy protections, priorities, and resources that will be allocated to protect the privacy of genomic data.	2 - Risks to relatives, especially around privacy, may be difficult to quantify and instead be based on qualitative considerations such as ethics and social harms, so establishing tolerances into an overall risk management strategy could potentially be set by looking to industry best practices. 10 - The value of IP to an organization is already assumed to be high (and may be more of a cybersecurity issue), so it may not receive as much analysis compared to other privacy risk factors.
GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	2	2	**1**	3	2	3	3	2	2	3	3	3	The organization's role in the processing ecosystem will guide requirements for data sharing and collaboration, since the organization will need to align its data process responsibilities with the requirements (or lack of requirements) found among the partners and third parties.	1,8,12 - Organizations may be able to establish privacy protections based on partnership expectations, while they work on defining their own risk tolerance levels. Changes in organizational ownership, partner engagement, technologies implemented, or data processing requirements will affect risk tolerances over time. 10 - Since an organization directly owns and protects its own IP, it will have already established the value and tolerances well in advance of ecosystem considerations.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	**1**	**1**	**1**	2	**1**	2	2	**1**	**1**	**1**	**1**	**1**	An organization's enterprise risk management processes help manage risks across all areas (e.g., legal, reputational, financial). Cybersecurity and privacy risks will also be incorporated as part of comprehensive risk management to help organizations appropriately assess risks to business continuity and operations.	1,3 - Cybersecurity risk management is built into the data life cycle to ensure the organization can complete its mission. 2,4,5 - Cybersecurity risk management addresses certain aspects of privacy risk management. 7 - Cybersecurity risk management processes can help protect trust and reputation. 10 - Cybersecurity risk management processes help identify and prioritize appropriate IP protections required to perform business operations. 12 - New technologies integrate appropriate cybersecurity and privacy risk management capabilities.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.	2	**1**	**1**	2	**1**	2	2	2	2	3	2	2	Organizations can prioritize addressing privacy risks (relatedness, consent) through governance-level oversight to establish policies and procedures required to enact these protections.	1,5 - Aspects of the data life cycle, such as data-in-use, also introduce risks. Other potential protections (such as homomorphic encryption) are addressed in other Subcategories. 2 - The governance body itself may need to understand the privacy risks to relatives from inferred data techniques, as this is largely a technical issue. 8 - Laws and regulations pertaining to the research ecosystem will also address privacy protections, such as HIPAA and GINA. 11 - Policies and procedures can help achieve an appropriate data diversity that may vary over time and across geographies.
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated.	2	2	2	2	2	2	**1**	3	2	**1**	2	2	Organization strategies define risk responses to manage and coordinate across partners any identified risks.	1,2,4,5,7,9,10 - These risk responses support the continuity of business operations by addressing protections and requirements for data quality, privacy, consent, reputation, IP, sample diversity, integration with new technologies, and legal risks.
GV.RM-P2: [Repeat]	2	2	**1**	3	2	3	3	2	2	2	3	3		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	**1**	2	**1**	2	2	2	2	2	2	3	2	**1**	Establishing lines of communication across the organization facilitates effective responses to genomic data risks introduced by suppliers or partners that could impact an organization's ability to meet genomic data processing objectives.	2,5 - All organizations in the genomic data supply chain manage privacy risks, including risks from aggregated and anonymized data that may be de-identified. 6 - Data access requirements apply to each organization in the supply chain. 7 - Reputation and trust are managed across all organizations processing the data. 12 - Organizations establish relationships with new technology providers to facilitate managing risks introduced by the technology solution.
CM.PO-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	2	2	2	**1**	**1**	**1**	**1**	**1**	2	3	**1**	2	Organizations will want to prioritize effective communication of any issues with data quality, provenance, access, and privacy to maintain trust across partners, donors, and customers that will encourage future participation. Communication across partners facilitates consistent incident response and recovery to a trusted operational state.	2,4,5,11 - Organizations can maintain the trust of donors and members of communities represented in research studies through proactive communication and notification of any issues that impact consent, privacy, or represented (or unrepresented) populations. Relatives will generally not be able to be notified. 8,10,12 - Researchers, owners of IP, and technology providers will benefit from communication across partners to manage privacy risks and help those using the data regain trust in the data quality, provenance, and research results.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.DE-P1: Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**1**	2	2	2	**1**	**1**	2	**1**	2	3	2	2	Data processing ecosystem risk management policies, processes, and procedures help promote consistency and trust in managing data quality, data provenance, privacy/consent, access controls, protection of IP, data diversity, and research data sharing, as well as legal/regulatory compliance.	2,4,5 - Identify where privacy risks to relatives or donors might arise in the genomic data processing ecosystem. Consent data will be treated as a high value and requires asset inventory and processing to know what data are subject to informed consent requirements and who can access that data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations. This may be prioritized due to the increased reach of data in research. The data processing environment will manage the appropriate degree of diversity. 12 - Data processing helps manage the effective, controlled sharing of genomic data across various technologies and even helps drive the requirements for technologies.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	2	2	**1**	2	2	**1**	**1**	2	**1**	**1**	3	2	Standardizing risk methodologies helps organizations establish consistency across partners (e.g., researchers), identify applicable laws and regulations, establish consistent access requirements for different user groups and data protection needs, and document requirements for protecting IP. Standardized practices help organizations to consistently develop and communicate incident criteria (i.e., DE.AE-08) for genomic data.	1,3 - Standardization helps ensure consistent data quality and provenance protections across the data processing life cycle and systems development life cycle. 2,4,5 - Standardization facilitates consistency in managing risk to privacy, reputation, and IP. 12 - Standardization ensures consistent risk management when integrating new technologies.
GV.RM-P1: [Repeat]	**1**	2	**1**	3	2	3	2	**1**	**1**	**1**	3	**1**		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	3	3	2	3	2	3	**1**	**1**	3	2	2	**1**	As organizations prioritize cybersecurity risk management practices, there may be opportunities to benefit from those improvements.	7 - Organizations with effective cybersecurity practices can use that capability to demonstrate their ability to be trusted by donors and other organizations and improve their overall market share and impact. 8 - Effective cybersecurity creates a strategic opportunity to demonstrate the trustworthiness of research results and as a research partner. 10 - Effective cybersecurity may be used to improve the marketing and trustworthiness of IP. 12 - New technologies that demonstrate effective cybersecurity practices will have strategic opportunities for marketing their product.

Table 6 presents the CSF and cross-walked PF Subcategories for the Roles, Responsibilities, and Authorities (GV.RR) Category. The CSF description for this Category is: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

Table 6. Govern: Roles, Responsibilities, and Authorities (GV.RR).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	2	2	2	2	2	3	**1**	2	**1**	2	2	2	Leadership that promotes accountability and responsibility will instill an awareness of, and compliance with, legal and contractual requirements, leading to improved cybersecurity outcomes and helping to achieve genomic data Mission Objectives.	7 - Reputation management starts at the highest level of the organization and is promoted by instilling a culture that values trust through trustworthy behaviors. 9 - Individuals in organizational leadership roles can be held legally responsible and accountable for organizational risk management strategies, decisions, and guidance that shape cybersecurity culture and compliance.
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	2	2	**1**	2	2	**1**	2	2	**1**	2	3	2	Those interacting with genomic data, including third-party stakeholders, will understand their responsibilities and training requirements to secure and protect the data throughout its life cycle. Roles and responsibilities establish the ability to hold people accountable for protecting the genomic data.	1 - Organizations manage data provenance and integrity by clearly articulating personnel responsibilities across the data life cycle, establishing accountability. 2,4,5 - Cybersecurity and privacy functions will be coordinated and supported by clear roles, responsibilities, and authorities, including all partners in the data life cycle. 3 - Clear roles and responsibilities empower personnel to effectively manage cybersecurity risks by setting clear

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														expectations. As an organization's risk posture changes over time, these roles and responsibilities also evolve to address emerging threats, such as insider risks, and to ensure the protection of any new types of information the organization may begin processing 9 - Laws and regulations may stipulate specific cybersecurity and privacy roles and responsibilities (for example, the CISO, ISSO, and Privacy Officer).
GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.	3	2	2	2	2	2	2	2	2	3	2	3	The workforce is directly responsible for data handling and requires clear guidance on roles and responsibilities, so they understand how their actions may affect genomic data processing and its provenance, privacy, and related aspects of its uses.	2,5,6,10 - The workforce will understand the value of the genomic data, including specific privacy considerations and any relevant IP. Role-based specifics of how to manage the data life cycle will be primarily addressed in the Control and Protect functions. 9 - The workforce will clearly understand their role in pertinent legal compliance issues. 12 - New technologies will include appropriate roles to reinforce privacy requirements.
GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders	3	2	2	2	2	2	2	2	**1**	3	2	2	Genomic data has unique characteristics (identifiability, relatedness) that require privacy protections. At the same time, data is widely shared, and ecosystem participants have varying	1,4,8,12 - Coordination acts to preserve original source (provenance) and privacy rights over the life cycle and across partners. Clear expectations and roles can help address deficiencies in environments where security and privacy are not typically priorities.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
(e.g., service providers, customers, partners).													standards and approaches to implementing protections. Enforcing standard protections across partners will help maintain consistent privacy protections in the ecosystem.	2,5 - Coordination across partners will help manage privacy protections specific to donors and relatives. 9 - Legal requirements merit additional prioritization as these issues have a risk profile (reputation, compliance) and can also be difficult to define as they may cover non-technical issues.
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	2	2	**1**	2	2	**1**	**1**	2	**1**	**1**	3	2	Organizations prioritize allocating resources to cybersecurity roles and responsibilities to implement and maintain cybersecurity capabilities that manage authorized access, protect IP, and ensure compliance with legal requirements.	1,3,6,8,10 - Organizations determine how many resources are needed to implement, monitor, and maintain cybersecurity capabilities to meet strategic goals and comply with policies. 2,4,5 - Organizations manage cybersecurity and privacy resources together to ensure that adequate resources are allocated to address both cybersecurity and privacy risk management priorities and needs.
GV.RR-04: Cybersecurity is included in human resources practices.	3	3	**1**	3	3	**1**	3	2	2	**1**	2	2	Human resource planning for cybersecurity takes into consideration important vectors, including insider threats and other personnel-related risks, and will be integrated with access control policies such as deprovisioning.	3,6,10 - These MOs require higher prioritization of personnel screening and management due to insider threat risks, including unauthorized access or IP loss. 8,9,11,12 - Organizations operating shared data environments or managing data stores implement HR policies to address personnel cybersecurity risks.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	2	3	2	2	3	2	2	3	3	3	3	2	Human resources practices will incorporate privacy requirements to ensure that personnel understand their responsibilities before entering a position and when leaving an organization. Combined with effective awareness and training, this practice can protect against personnel accessing or revealing sensitive information specific to the organization, such as IP or the use of new technologies.	1,6,12 - Procedures help enforce consistent security practices to manage provenance, ensure data quality, and restrict access. Access controls need to be updated for staff turnover. 4 - Procedures support access management, aligned with consent requirements. 7,9 - HR practices help create a culture of trust in organizations and establish their reputation. Before participating in genomic data activities, potential donors want to know they can trust organizations with their genomic data and the workforce within those organizations charged with safeguarding the data.

Table 7 presents the CSF and cross-walked PF Subcategories for the Policy (GV.PO) Category. The CSF description for this Category is: Organizational cybersecurity policy is established, communicated, and enforced.

Table 7. Govern: Policy (GV.PO).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	**1**	**1**	**1**	**1**	**1**	2	**1**	**1**	**1**	**1**	**1**	**1**	Policies establish organizational expectations, processes, responsibilities, and priorities that embed and enforce legal, regulatory, security, and privacy requirements.	1 - Policies incorporate data quality and provenance requirements. 2,4,5 - Policies address privacy and consent requirements, including protecting relatives' privacy. 3,6,10 - Policies define required risk management activities, access controls, and IP protections. 11 - Policies help enable and preserve sample diversity. 12 - Policies enforce cybersecurity requirements for technology solutions.
GV.PO-P1: [Repeat]	**1**	**1**	**1**	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2		
GV.PO-P6: [Repeat]	2	**1**	**1**	2	**1**	2	2	2	2	3	2	2		

Subcategory	**1. Data**	**2. Relatives**	**3. Risks**	**4. Consent**	**5. Donors**	**6. Access**	**7. Trust**	**8. Research**	**9. Legal**	**10. IP**	**11. Diversity**	**12. Tech**	**General Rationale**	**Mission Objective Specific Considerations**
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	**1**	2	**1**	**1**	2	2	2	2	**1**	2	2	**1**	Due to the dynamic nature of genomic data processing and ecosystems, policies will be updated frequently to address new threats, uses, technologies, and requirements.	1,3,6,8,10 - Policy updates help to address newly identified cybersecurity risks to data quality, provenance, access control, research environments, and IP. 2,4,5 - Policy updates help address changes to privacy or consent requirements, threats, and uses, as well as advancements in privacy protections. 12 - Policy updates help manage cybersecurity risks introduced by the use of new technologies.
GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	2	**1**	**1**	2	**1**	2	**1**	2	**1**	3	2	2	The genomic research landscape is quickly evolving, expanding data sharing, leveraging new technologies, and operating in new environments. Organizations will regularly re-assess their privacy risks to both donors and relatives, including legal, technical, and social risks.	2,3,4,5 - Conduct privacy risk assessments to assess the impact that changes in technology and regulations may have. Privacy, consent, and relatedness issues may impact dignity loss, discrimination, loss of trust, or loss of autonomy because of unanticipated revelation of health conditions of donors or their kin/progeny. 6 - Automated continuous monitoring of data access is expected to maintain situational awareness and

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														compliance with data breach detection and reporting requirements. 11 - Privacy risks to data sets and sample diversity could impact decisions to share those data sets with certain partners.
GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	2	2	2	3	2	3	2	3	2	3	3	3	Lessons learned can address current shortcomings, reinforce improvements, and inform future changes to improve the privacy and security posture of an organization. This includes updates to training and awareness materials. Failure to incorporate lessons learned may indicate negligence and destroy trust.	12 - An example of incorporating lessons learned from new technologies is the implementation of safeguards against potential problematic data actions from new de-anonymization techniques that could be used to access or aggregate data of a discriminated population.

Table 8 presents the CSF and cross-walked PF Subcategories for the Oversight (GV.OV) Category. The CSF description for this Category is: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

Table 8. Govern: Oversight (GV.OV).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	2	3	2	3	3	2	2	3	2	2	3	3	Adjustments ensure that priorities and investments are effective in managing the changes in the risks to the genomic data and processing environment.	7,9,10 - Ensure that the strategy reflects priorities to manage trust, reputation, legal compliance, and IP protections.
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	2	2	**1**	3	2	2	2	2	2	3	3	2	The dynamic nature of the genomic data processing ecosystem requires organizations to review changes to requirements and risks that will be incorporated into their cybersecurity risk management strategy.	1 - Audit findings confirm compliance requirements for data-sharing arrangements among third parties so that protections are met throughout the life cycle. 3 - The cybersecurity risk management strategy dictates the requirements for cybersecurity and risk assessment and will be adjusted as risk assessment findings identify risks.
GV.RM-P1: [Repeat]	**1**	2	**1**	3	2	3	2	**1**	**1**	**1**	3	**1**		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	3	3	**1**	3	2	2	2	3	2	3	3	2	Measure, review, and adjust cyber risk management processes to address cybersecurity risks to genomic data as they are identified.	3 - The risk assessment process is adjusted to identify and address deficiencies in the overall cybersecurity risk management program. 10 - Outcomes from performance evaluations ensure appropriate adjustments are made to protect IP.

Table 9 presents the CSF and cross-walked PF Subcategories for the Cybersecurity Supply Chain Risk Management (GV.SC) Category. The CSF description for this Category is: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

Table 9. Govern: Cybersecurity Supply Chain Risk Management (GV.SC).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	**1**	2	**1**	2	2	2	2	2	2	2	2	**1**	A supply chain risk management program helps an organization integrate data protections, risk assessments, access controls, legal requirements, IP protections, and new technology assessments across all partners involved in the genomic data life cycle.	2,4,5 - All organizations in the genomic data supply chain preserve privacy and ensure that consent travels with privacy data. Privacy risks may arise even when processing data that has been aggregated or de-identified (including anonymized data). 7 - Manage reputation and trust across all organizations in the data supply chain that process genomic data. 11 - Preserve sample diversity throughout the supply chain.
ID.DE-P1: [Repeat]	**1**	2	2	2	**1**	**1**	2	**1**	2	3	2	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	**1**	2	**1**	2	2	**1**	2	**1**	**1**	2	2	2	Those interacting with genomic data, including third parties, will understand their responsibilities in securing the data. Defining roles and responsibilities with external partners and suppliers helps align their practices with the organization's cybersecurity risk management requirements, which include training, risk assessment, and privacy.	1,3,6 - Enforce consistency in managing data quality, provenance, risk assessment, and access controls. 2,4,5 - Consistently communicate privacy responsibilities across the workforce, third-party stakeholders, partners, and suppliers. 8,10,12 - Coordinate consistent expectations across researchers, partners, and new technology providers for genomic data and IP protections. 9 - Laws and regulations stipulate specific cybersecurity and privacy roles and responsibilities.
GV.PO-P3: [Repeat]	3	2	2	2	2	2	2	2	2	3	2	3		
GV.PO-P4: [Repeat]	3	2	2	2	2	2	2	2	**1**	3	2	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	2	2	**1**	2	2	2	2	2	2	3	2	2	Genomic data life cycles include sharing between many partners, introducing supply chain risk. Organizations develop cyber supply chain risk assessment processes tailored to meet privacy, data quality, provenance, data access, and diversity requirements. Independent risk assessments verify an organization's trustworthiness in handling sensitive data.	1 - Genomic data relies on the supply chain to maintain data quality and provenance, regularly assessing and addressing deficiencies. 2,4,5 - Privacy protections for donors and relatives are considered and assessed across the supply chain, verifying that consent travels with the data. 3 - Risk assessments address and incorporate supply chain risks to ensure protection of genomic data. 12 - Results from risk assessments of new technologies are integrated into the overall supply chain risk management process.
ID.DE-P2: [Repeat]	**1**	2	**1**	3	**1**	2	2	2	2	3	2	2		
GV.SC-04: Suppliers are known and prioritized by criticality.	**1**	2	2	2	2	2	2	2	2	3	2	2	Because of the complexity and value of the genomic data life cycle, organizations prioritize suppliers who implement cybersecurity and privacy protections for genomic data.	1,6,10 - Organizations prioritize suppliers who maintain data quality, provenance, access controls, and IP protections. 2,4,5 - Organizations prioritize suppliers who effectively implement privacy requirements, including managing consent. 3,7 - Risk assessments verify the trustworthiness of suppliers.
ID.DE-P2: [Repeat]	**1**	2	**1**	3	**1**	2	2	2	2	3	2	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	**1**	**1**	2	**1**	**1**	2	2	2	2	2	2	2	Organizations use contracts to define and enforce genomic data processing requirements, including data quality, provenance, data access, privacy, consent, IP protections, sharing agreements, sample diversity, and new technology requirements.	2,4,5 - Contracts help manage and communicate privacy and consent requirements that need to travel with the data. 9 - Contracts provide the legal avenue for enforcing agreements. 12 - When contracts are used with technology suppliers, appropriate cybersecurity language will be included to enforce consistency in risk management.
ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	**1**	2	2	2	**1**	2	2	**1**	**1**	3	3	2	Contracts manage expectations across parties including data quality, provenance, privacy/consent, access controls, IP protection, data diversity, and legal/regulatory compliance.	4 - Contracts are a primary mechanism for establishing expectations for managing consent and ensuring that consent travels with the data. 7 - Contracts ensure that external risk management activities that foster trust are supported by stakeholders. 12 - Secure technologies track and enforce data processing requirements to implement contractual agreements.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	**1**	2	**1**	2	2	2	**1**	2	2	3	2	**1**	The ability to assess the trustworthiness of suppliers to handle genomic data in advance of using their services reduces overall risks, including cybersecurity risks.	1,3,6,8 - Assess risks to data quality, provenance, and access control before using any genomic data organization as part of the supply chain. 2,4,5 - Determine whether suppliers implement effective privacy practices, including managing consent. 12 - Technology providers will want to assess any supplier dependencies and ensure that they are able to demonstrate their trustworthiness as a supplier.
ID.DE-P1: [Repeat]	**1**	2	2	2	**1**	**1**	2	**1**	2	3	2	2		
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	2	2	**1**	2	2	2	2	2	2	2	2	2	Ongoing supplier risk assessments monitor compliance with genomic data protection requirements, including data quality, privacy, consent, data access, legal compliance, IP protections, sample diversity, and risks from new technologies.	2,4,5 - Monitoring can confirm that consent and other privacy requirements are managed appropriately. Monitoring may be the best way to determine any impact on relatives' privacy. 3,6,9,12 - Supplier risk assessment and ongoing monitoring address changes in threats, technologies, processes, legal or contractual requirements, and other risk factors.
ID.DE-P2: [Repeat]	**1**	2	**1**	3	**1**	2	2	2	2	3	2	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.	2	3	2	2	2	2	3	2	2	3	2	2	These assessments verify that partners meet obligations for maintaining data quality, provenance, donor consent and privacy, access control, IP protection, and legal and regulatory compliance.	7 - Assessments can be used as a mechanism for verifying and demonstrating trust between stakeholders. 12 - Assess technologies for effectiveness in managing privacy requirements.
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	2	3	2	3	3	2	3	3	2	2	3	2	Involve suppliers in incident planning, response, and recovery to identify points of coordination across the genomic data processing life cycle and manage changes as they occur. Document expectations for supplier and third-party incident response capabilities in contracts and other types of agreements consistent with GV.OC-03 and GV.SC-05.	1,6,10 - Coordinate across partners to maintain provenance, data quality, data access, and IP protections during response and recovery operations. 2,4,5 - Plans define and communicate partners' privacy-related response and recovery responsibilities and associated privacy requirements. 9 - Involve all appropriate parties in response and recovery to support legal requirements for processing genomic data. 12 - Organizations using new technologies determine when suppliers need to be involved in response and recovery activities.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	**1**	2	**1**	2	2	2	2	2	2	3	2	2	Manage the cybersecurity and enterprise risks introduced by suppliers throughout the life cycle to determine any impact on genomic data quality, data access, reputation, research integrity, legal compliance, and sample diversity.	2,4,5 - Organizations involved in the genomic data supply chain comply with privacy and consent requirements. Privacy risks may arise even when processing data that has been aggregated or de-identified (including anonymized data). 12 - The risks introduced by suppliers of new technologies are monitored and managed throughout the product life cycle.
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	2	**1**	2	2	**1**	**1**	2	2	2	2	2	2	Organizations include provisions in agreements and contracts to ensure that partners adhere to data protection, data sharing, consent, and disposal requirements at the conclusion of the agreement. Failure to protect data after the agreement ends may result in unauthorized access along with legal or regulatory consequences.	2,4,5 - If data is not appropriately protected after the agreement ends, it may impact relatives' privacy as well as donors and fail to follow consent requirements. 7,8 - Partners who fail to protect data after the agreement ends will not be trusted in the future. 12 - Supporting technologies incorporate ways to verify that there is no residual data access after use and agreements end.

Table 10 presents the CSF and cross-walked PF Subcategories for the Asset Management (ID.AM) Category. The CSF description for this Category is: Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Table 10. Identify: Asset Management (ID.AM).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-01: Inventories of hardware managed by the organization are maintained.	2	3	2	3	2	**1**	3	2	2	**1**	2	**1**	Managing hardware inventories, including any unauthorized hardware across the genomics supply chain (sequencers or IoT devices), increases organizational situational awareness.	1,8 - Monitor genomic data processing hardware to prevent issues with provenance or data quality. 6,12 - Hardware inventories help identify new technologies and unauthorized hardware that may be used for unauthorized access to sensitive data. 9 - Legal requirements may include maintaining an asset inventory as part of standards of practice or regulatory requirements. 10 - Protect IP information from all potential threat vectors, including hardware.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-P1: Systems/products/ services that process data are inventoried.	**1**	2	**1**	2	2	**1**	2	2	2	**1**	**1**	2	Inventories identify threats, vulnerabilities, privacy problems, and data origins (provenance), and they inform quality management across the data life cycle, as well as access requirements, legal and regulatory risks, and the need for additional technologies to support data protections.	4 - Inventory the data to understand data types, consent requirements, and applicable regulations; inventory the systems to understand data processing across systems and how consent is shared. 8 - Data process inventories inform research data management by identifying and tracking data collection and sharing processes.
ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/ services and components (e.g., internal or external) that process data are inventoried.	**1**	2	**1**	2	2	**1**	3	2	2	**1**	**1**	3	Ownership helps identify data origins (provenance), data access management requirements, and legal and regulatory risks. Owners understand data privacy requirements including consent, data retention, access controls, and data diversity requirements, as well as their role in maintaining trust among partners.	2 - Situational awareness of ownership helps ensure data are accessed and shared appropriately; restricting who has access may help restrict the ability to identify relatives. 3 - Roles help identify potential risks from external parties. 10 - Ownership establishes and traces provenance, who can access the IP, how to protect the IP and related business interests, and who is responsible for protecting the IP.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	**1**	3	**1**	2	3	2	2	2	**1**	**1**	2	2	Understanding where data is processed helps identify risks to data quality, provenance, data privacy, consent, IP, and related legal and regulatory compliance resulting from cloud processing, third-party risks, and geographic risks. Manage data sharing, data diversity requirements, and access authorization across ecosystem boundaries.	4 - The data processing environment may influence donors' decisions regarding consent. For example, they may accept data processing in their home country but not in locations with differing privacy standards, or they may be comfortable with data being processed in-house but uncomfortable with data being processed in a cloud environment. 9 - International data sovereignty and privacy rights may impose unique challenges that require stricter compliance with laws and regulations; location determines applicable laws, regulations, policies, and standards.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	**1**	2	**1**	2	2	**1**	2	**1**	2	**1**	2	**1**	Software and services used in genomic research settings represent a broad attack surface. Maintaining updated inventories helps identify unauthorized software and manage risks to data quality, provenance, IP protections, and platforms. Many organizations require a software bill of materials (SBOM).	1,3,6 - Software and services represent a primary attack vector for unauthorized access and data breaches. 2,5 - Inventories are used to identify potential harms from software used to process relatives' and donors' data. 10 - Inventories of software interacting with IP or of the IP itself provide an awareness of potential attack vectors. 12 - Software and systems delivered as part of new technologies represent a significant risk.
ID.IM-P7: [Repeat]	**1**	3	**1**	2	3	2	2	2	**1**	**1**	2	2		
ID.IM-P1: [Repeat]	**1**	2	**1**	2	2	**1**	2	2	2	**1**	**1**	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	**1**	**1**	2	**1**	**1**	**1**	3	**1**	2	**1**	2	**1**	As the processing environment of genomic data becomes more complex, mapping network communications and interconnections provides the basis to determine appropriate access authorizations, manage data provenance, identify potential risks, and provide accurate information for security control implementation.	1,6,8 - Network communications and data flows help track where and how genomic data is being used, along with any impact on data quality, provenance, and access throughout the genomic data life cycle. 2,4,5 - Organizations track where donors' and relatives' data are processed to manage privacy requirements, including consent, which travels with the data. 10 - Mapping data flows can help identify threats to IP everywhere it is processed. 12 - Tracking data flows for new technologies integrated with genomic processing helps determine where risks to data might be introduced.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/ services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/ services.	**1**	2	**1**	2	2	**1**	2	2	**1**	2	2	2	Data process mapping tracks where data comes from, where it goes, and how it is processed in the life cycle, providing an overarching understanding of risks to data quality, provenance, privacy, and IP. Mapping helps manage data sharing across collaborators, including data access management and monitoring, as well as data diversity management.	2,4,5 - Privacy risk directly correlates to data processing and cannot be evaluated without understanding the data actions and data flows. Informed consent means understanding data processing activities and locations, privacy and security protections, and what consent will mean for the donor. 9 - Data processing inventories support compliance with laws and regulations, understanding what schemas apply (e.g., GDPR, HIPAA), and understanding citizenship for data subjects (e.g., GDPR, state laws). 12 - Technologies may help bring people to the data rather than sharing the data across multiple internal and external environments. Manage the inventory across the range of technologies and environments: cloud, private networks, locations, etc.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-04: Inventories of services provided by suppliers are maintained.	**1**	2	2	2	2	**1**	3	**1**	2	2	2	2	Organizations identify and maintain inventories of services provided by suppliers that participate in the genomic data life cycle to include them in asset management processes. Most genomic organizations rely on external data systems to perform data processing and analysis, storage of large datasets, or archival/retrieval of the data in repositories for shared research.	1,3,6,12 - Genomic data processing is becoming increasingly more complex and interconnected (e.g., genomic data banks and research initiatives). Service inventories help identify potential risk sources introduced by suppliers. 4 - Inventorying services helps manage consent, which travels with human genomic data. 8 - Service inventories help research institutions understand how data may be impacted by other services in data analysis pipelines. 10 - IP in the form of software or data may be a high-value target and is at risk from unauthorized or shadow services associated with third-party suppliers.
ID.IM-P2: [Repeat]	**1**	2	**1**	2	2	**1**	3	2	2	**1**	**1**	3		
ID.IM-P7: [Repeat]	**1**	3	**1**	2	3	2	2	2	**1**	**1**	2	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	**1**	2	**1**	2	2	**1**	2	2	2	**1**	2	2	Organizations prioritize assets to manage risks to genomic data. Factors include risks to privacy, consent, unauthorized access, research outcomes, IP, and availability (e.g., services).	1,6 - Data prioritization and classification are inherently part of managing data provenance, integrity, and access control activities. 2,5 - Organizations prioritize privacy attributes when determining the value of genomic data (in addition to business- and mission-related values). 9 - Legal requirements vary across geographies and require comprehensive classification efforts. 10 - For genomic research, the IP may be the data itself (or derivatives of its use).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	**1**	**1**	**1**	**1**	**1**	**1**	3	**1**	**1**	**1**	**1**	2	Maintaining inventories of data and associated metadata is the basis of tracking the provenance of sensitive data (e.g., relatives, donors) throughout the data life cycle and provides organizations with traceable links to ownership, use, and protections.	1 - Data provenance management requires maintaining data and metadata inventories. 2,5 - Metadata helps identify security and privacy concerns for relatives and donor data where risks or harms can occur from secondary associations. 4 - Consent in the form of either data or metadata will be inventoried and associated with its respective genomic information at all stages of processing. 6 - Access control is dependent on knowing the type, classification, and location of data throughout its life cycle in the ecosystem. 8,9,10 - Understanding the types of data processed drives cybersecurity and legal protections in research environments, for privacy data, and for IP.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-P6: Data elements within the data actions are inventoried.	**1**	2	**1**	2	2	2	2	2	2	2	**1**	2	Data element inventories help define potential risks to data quality, provenance, data access, legal compliance, and data sharing. Metadata may be a source of privacy-related information. In the case of a clinical study, data elements are likely to be pre-determined prior to starting a study and then reused thereafter.	2,4,5 - Privacy risk directly correlates to data processing and cannot be evaluated without understanding the data elements, which may contain information pertaining to relatives, donors, and consent. Consent practices can be managed at the data element level when necessary. 8 - Data management is part of managing research. Research activities may have increased or specialized data handling requirements. 11 - Data elements may determine the degree of diversity (i.e., do you have enough data to make a determination?) and provide statistical confidence. Genomic sample diversity enables researchers to identify genetic variants with greater statistical confidence, and allows for a more comprehensive and inclusive understanding of diverse populations.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles.	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	**1**	2	2	Genomic data processing ecosystems include a range of systems, hardware, software, services, and data that will be managed over the entire life cycle to identify redundancies, vulnerabilities, noncompliance, and unauthorized access. Life cycle management includes a review of disposition processes and maintenance (including remote) to secure genomic data, environments, and the privacy of individuals while incorporating insider threat program requirements.	1 - Data quality and provenance depend on managing systems and data across the entire life cycle. 2,4, 5 - Cybersecurity privacy considerations span the entire data life cycle, including acquiring, aggregating, and disposing of data according to consent and other privacy requirements. 3,9 - Implementing life cycle processes and activities helps manage and address the risks associated with processing genomic data while also reflecting laws or guidance that stipulate patching outdated software or migration away from unsupported hardware and software. 6 - Managing systems includes identifying redundant or non-compliant systems that may expose systems or data to unauthorized access. 8 - Research environments often include outdated assets that may require compensating controls to protect the data. 10 - IP protections will be confirmed throughout the life cycle to prevent unauthorized tampering or disclosure during system development, upgrade, migration, or disposal.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.MA-P1: Maintenance and repair of organizational assets are performed and logged with approved and controlled tools.	2	3	3	3	3	3	3	3	3	2	3	3	Maintenance and repair of assets support processing and protecting genomic data as part of managing access and having audits of any maintenance and repair.	1,4,5,6,10 - Logging maintenance and repairs impacts an organization's ability to manage data, protect IP, and maintain quality, using audits of such activities to establish and trace data ownership and provenance. Logging also supports tracking who accessed privacy data to manage consent.
PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	2	3	3	3	3	2	3	3	3	2	3	3	Implementing approved remote maintenance access supports appropriate use of data to prevent unauthorized access, manage authorized access, and prevent unauthorized modifications to sensitive information as part of protecting genomic data.	1,4,9 - Access (whether authorized or unauthorized) as part of remote maintenance to devices and machines needs to be controlled to prevent people from accessing, modifying, or deleting sensitive information and support appropriate use of data consistent with consent or legal/regulatory compliance.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.DM-P5: Data are destroyed according to policy.	**1**	**1**	2	2	**1**	**1**	2	2	**1**	2	2	2	This Subcategory implements a specific use case for CT.DM-P4. Data will be deleted when requested by donors in accordance with retention policies and secure removal practices as well as applicable laws and regulations.	2 - Data destruction limits the long-term ability to infer associations with relatives. 4,5,7 - Implement consent and foster donor trust by deleting data in accordance with individual preferences and the relevant retention schedule. 6 - Deletion in accordance with retention policies supports restricting unauthorized access. 11 - Failure to delete data impacts trust in under-represented populations and makes it less likely that a diverse group of donors will participate.
CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	**1**	2	2	2	2	2	3	3	2	3	3	**1**	Alignment of data and system life cycles helps integrate data management, data sharing, and data processing requirements while addressing risks as data is shared, aggregated, and changed.	1, 3 - Data and system life cycles integrate risk management processes and protect data quality and provenance. 4,12 - Consent will be managed throughout data and system life cycles, with special care to address data aggregation and possible re-assessment when technologies enable new processing capabilities and privacy engineering practices. 9 - Governance and regulatory compliance may focus on an organization’s ability to manage data and system life cycles.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.DS-P3: Systems/products/ services and associated data are formally managed throughout removal, transfers, and disposition.	**1**	2	2	3	**1**	2	3	3	2	2	3	2	Part of careful management and control of genomic data and keeping that data secure is knowing what systems data is on and making sure data is appropriately destroyed once it is no longer needed. Managing genomic data according to risk strategies protects provenance and data quality and maintains data protections as assets move, representing an accountability measure that supports trust of organizations by individuals.	1,10,12 - This helps establish and trace data and IP ownership and provenance to manage data throughout its life cycle. 8 - Security to protect against data leaks is needed at all steps in research, from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data. As more researchers gain access to genomic data, enhanced or additional protections may be required. 9 - Organizations will comply with legal and regulatory requirements for destruction and proper disposal. 12 - Organizations implementing new technologies manage both the disposal of old devices and the acquisition of any new devices to protect the data.

Table 11 presents the CSF and cross-walked PF Subcategories for the Risk Assessment (ID.RA) Category. The CSF description for this Category is: The cybersecurity risk to the organization, assets, and individuals is understood by the organization.

Table 11. Identify: Risk Assessment (ID.RA).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	**1**	2	**1**	3	2	**1**	2	**1**	2	**1**	3	**1**	Organizations prioritize vulnerability assessments to proactively identify and evaluate vulnerabilities that may introduce cybersecurity risks and help mitigate known threats by identifying potential attack vectors that may impact genomic data.	1,6 - Data provenance, integrity, and access protections begin with identifying and addressing system vulnerabilities that might compromise genomic data throughout its life cycle. 2,5 - Vulnerability assessment reduces potential harms to donors and relatives by protecting their data from threats such as unauthorized access or data breaches. 3,8,10,12 - Vulnerability management provides a baseline for managing risks to genomic data that will be applied in research environments, when protecting IP, and for assessing risks from new technologies.
PR.PO-P10: A vulnerability management plan is developed and implemented.	2	3	**1**	3	3	3	3	3	3	3	3	2	The vulnerability management plan documents how the organization identifies, prioritizes, and tracks the remediation of vulnerabilities and will be coordinated across partners through contracts and agreements.	3 - These plans provide the vulnerability inputs to risk modeling and management. 4,5 - Vulnerabilities may directly impact privacy and consent and will be tracked comprehensively to manage associated risks. 12 - The plan will include provisions for how to manage vulnerabilities introduced in new technologies and ensure that contracts with technology providers incorporate sufficient support to ensure

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														remediation of vulnerabilities throughout the technology life cycle.
ID.RA-02: Cyber threat intelligence is received from information-sharing forums and sources.	3	3	**1**	3	3	3	3	2	2	2	3	2	Cyber threat intelligence (CTI) informs organizations of specific threat actors and attack vectors against genomic information. Organizations and research consortiums can monitor CTI to stay abreast of emerging threats in a rapidly evolving field. Genomic CTI may be identified from relevant forums such as the BIO-ISAC (Bioeconomy Information Sharing and Analysis Center).	3 - CTI provides the threat input to risk modeling and management. 7 - Receiving and sharing CTI as part of a common effort to address threats collectively can build trust among genomic community participants. 10,12 - Monitoring CTI can provide an organization with insight into potential threats to its IP or new technologies.
ID.RA-03: Internal and external threats to the organization are identified and recorded.	**1**	2	**1**	3	2	2	2	**1**	2	**1**	3	2	An overall program to identify and maintain an inventory of threat actors (either by CTI feeds or active threat hunting) allows organizations to more accurately assess risk and implement effective controls to protect genomic data.	1,3,10 - Maintaining awareness of likely threat actors targeting the organization informs effective practices for risk reduction and protection of high-value assets (such as genomic data and related IP). 7,9 - The consistent use of CTI demonstrates a level of due diligence and adherence to legal requirements that benefits the organization's reputation in the event of cyberattacks or data breaches. 8,12 - The use of the emerging and rapidly evolving technology typically found in

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														research requires vigilant identification of new threats and tactics, techniques, and protocols (TTPs).
ID.RA-P3: Potential problematic data actions and associated problems are identified.	**1**	**1**	**1**	2	**1**	2	2	3	**1**	**1**	2	**1**	Problematic data actions (PDAs) may affect source rights and privacy rights over time and can include misuse, improper sharing, and other things impacting data quality, provenance, privacy/consent, access controls, protection of IP, data diversity, and research data sharing/outcomes, as well as legal/regulatory compliance.	2,4,5 - PDAs may include combining data sources that could create privacy harms impacting donors and/or relatives and violate informed consent. 10 - Evaluate the impact on IP from PDAs, including those introduced by open-source software. 11 - Diversity is not just in collection. Changes in the data through processing may affect the ability to maintain data diversity. Specific populations or individuals can have differing views on data processing and what constitutes a PDA. 12 - Technologies may play a role in managing risk from PDAs related to data sharing. Use of technology may also introduce PDAs and associated risks.
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	2	2	**1**	2	2	2	2	**1**	2	**1**	2	**1**	Organizations manage risk by understanding how exploited vulnerabilities can potentially impact operations and genomic data participants (donors and relatives). Understanding this impact helps organizations make risk determinations (asset-	1,2,5 - The potential impacts of exploited vulnerabilities can impact the organization as well as donors and relatives since genomic data is a unique identifier. By identifying and understanding the potential impact on the organization and individuals, organizations can assess the likelihood and impact of risk scenarios. 3 - Likelihood and impacts serve as inputs in modeling and managing risks.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													threat pairing) and assess the costs and benefits of security capabilities.	8,12 - External stakeholders involved in broader research and data-sharing initiatives will be considered when identifying potential impacts, including those introduced through new technologies.
ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	2	**1**	**1**	2	**1**	2	2	3	**1**	2	2	**1**	Risk assessments will determine the PDAs' likelihood and potential impact on genomic data to prioritize risk responses and track changes in risk due to emerging capabilities, evolving threats, or unanticipated changes in how data can be used.	2,4,5 - If PDAs impact consent or the privacy of donors or relatives, that risk will be assessed and managed, considering secondary risks (e.g., to relatives or downstream in managing consent). 8 - Understand the impact on the research, including research environment, data, and outcomes. 9 - Monitor the PDAs' impact on legal requirements. 12 - Assess PDAs to identify concerns with data processing activities, use of technologies, and data-sharing activities.
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	**1**	**1**	**1**	2	**1**	2	2	**1**	2	**1**	2	**1**	Organizations assess and analyze threats, vulnerabilities, likelihoods, and impacts to obtain inputs that form the basis of calculating risk, developing models, and prioritizing responses proportionate to the risk and the value of the genomic assets under consideration.	1,3,10 - Organizations prioritize resource allocations and risk responses for high-value assets (particularly genomic data and IP) based on risk models that are developed from these inputs. 2,4,5 - Inherent risk from potential privacy harms to relatives and donors is considered as part of the risk equation. 8,12 - Threats and impacts to the organization and stakeholders from data-sharing agreements and new technologies are inputs for inherent risk determination.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.RA-P4: [Repeat]	2	**1**	**1**	2	**1**	2	2	3	**1**	2	2	**1**		
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	**1**	2	**1**	3	2	2	2	**1**	2	**1**	3	2	Appropriate risk responses will address risks to genomic data, applying criteria from the organization's vulnerability management plan to decide whether to mitigate, transfer, accept, or avoid risks identified, as well as applicable cybersecurity safeguards to implement.	1 - Risk response planning helps coordinate the activities required (internal and external) to manage data quality and provenance when events occur. 2,4,5 - Cybersecurity-related risk responses for privacy harms to donors and relatives are understood, documented, and prioritized. 8 - Due to the broadness of the research community, researchers consider the entire ecosystem when developing effective risk responses. 9 - Risk responses consider any legally-required response activities, including tracking progress of such activities and data breach notification. 10 - Risk responses will ensure that appropriate protections are in place for IP.
ID.RA-P5: Risk responses are identified, prioritized, and implemented.	2	2	**1**	3	2	2	2	3	3	2	3	2	Effective risk response can identify relevant threats related to data quality and provenance, unauthorized access, loss of IP, and legal requirements, preventing further issues and improving trust between partners.	2,4,5 - Response includes appropriate notification when consent or privacy of donors or relatives is impacted. 12 - Use of technologies will document potential issues that need to be evaluated during response and recovery operations. Notification of technology providers and consumers will be prioritized.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	**1**	2	2	2	2	2	3	3	2	**1**	3	2	Organizations use a security impact assessment process to evaluate the impact of changes to genomic data processing. Managing changes and exceptions using risk modeling and responses provides an organization with a consistent and traceable process to update its risk posture, detect unauthorized changes, control authorized updates, and minimize unintended consequences from unauthorized changes.	1 - Risks to data quality and provenance will evolve and will be tracked and periodically reviewed for security implications. 2,4,5 - Changes in risk determinants related to privacy harms require formal review, testing, and approvals to remain relevant and effective. 6 - Reviewing changes in configuration profiles and protections supports organizational change management needed for access control requirements. 9 - Organizations monitor changes to laws and regulations to determine cybersecurity impacts. 10 - Organizations monitor the impact of changes that may affect or introduce risks to IP.
PR.PO-P2: Configuration change control processes are established and in place.	**1**	3	2	3	2	2	3	3	3	3	3	**1**	Establishing configuration change control processes ensures that genomic data processing remains intact as intended and that changes are evaluated for new risks. Configuration change control processes can also support preventing unauthorized data changes and ensure that when data processing life cycle changes are made, privacy	1,3,6 - Change control reduces the risk of unauthorized changes that may impact data access, quality, or provenance and ensures that risks from new changes are evaluated. 2,4,5 - Change control will monitor for changes that may impact the effectiveness of privacy controls and the ability to manage consent. 12 - Change control for new technologies will be used to ensure unauthorized

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													safeguards of genomic data don't "break."	changes don't occur that introduce additional privacy or security risks.
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	2	2	2	3	2	3	3	3	3	**1**	2	2	Vulnerability disclosure programs provide a way for organizations to respond to vulnerabilities discovered by external parties. Since genomic processing requires collaboration across organizations, a process for responding to identified vulnerabilities helps coordinate response across partners.	1,10 - Organizations protecting data quality, provenance, and IP will want to quickly address identified system vulnerabilities. 3 - Effective risk management involves consistently managing vulnerability disclosures and implementing appropriate protections. 8,11,12 - Environments with broad attack surfaces, emerging technologies, or multiple stakeholders will benefit the most from coordinated response to vulnerabilities by external sources.
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	2	3	3	3	3	2	3	3	2	2	3	**1**	Authenticity and integrity testing assures that the system has not been tampered with and that it implements the minimum acceptance criteria and functionality required for security and privacy objectives. With the complex interconnection of systems used in genomic processing, including open-source software, organizations can confirm the provenance of software assets using SBOMs.	1 - Hardware and software require authenticity testing to identify tampered assets that may threaten data quality or provenance. 2,4,5 - Systems may be tampered with to attempt unauthorized access to privacy-related information. 8,12 - Research and new technologies may include a wide range of equipment, proprietary hardware, and IoT devices. Testing assures that minimum acceptance criteria are met. 10 - Testing of hardware and software prior to use can identify potential vulnerabilities (e.g., malicious code,

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														backdoors) that can be exploited for attacks on IP.
PR.DS-P8: Integrity-checking mechanisms are used to verify hardware integrity.	2	3	2	3	3	3	3	3	3	3	3	3	Integrity-checking mechanisms may be helpful as a data security best practice for achieving data quality or provenance.	1 - Integrity checking for hardware may be prioritized to manage data quality and chain of provenance. 12 - Emerging technologies may use integrity-checking mechanisms and ensure that hardware devices are from approved sources, noting that laws may ban the use of hardware from certain nation states.
ID.RA-10: Critical suppliers are assessed prior to acquisition.	**1**	2	**1**	2	2	2	2	2	2	3	2	2	A supplier risk assessment allows an organization to identify potential problems from external assets (e.g., foreign ownership, control, or influence) prior to their use in the genomic processing environment. Effective risk management will assess any impact from critical suppliers in an organization's supply chain, including impacts to the genomic data supply chain.	1,2,4,5 - Supplier risk assessments help identify problematic assets or services, including any risks to data quality, provenance, consent, and donors' or relatives' privacy. 7 - Obtaining unsecured, counterfeit, or unauthentic supplies puts the organization's trustworthiness and reputation at risk. 12 - New technologies may include hardware and software from third-party suppliers that will be assessed prior to acquisition, particularly when they are produced by a supplier in a location of concern.
ID.DE-P2: [Repeat]	**1**	2	**1**	3	**1**	2	2	2	2	3	2	2		
ID.DE-P5: [Repeat]	2	3	2	2	2	2	3	2	2	3	2	2		

Table 12 presents the CSF and cross-walked PF Subcategories for the Improvement (ID.IM) Category. The CSF description for this Category is: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.

Table 12. Identify: Improvement (ID.IM).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-01: Improvements are identified from evaluations.	3	2	**1**	3	2	2	3	3	2	2	3	2	Continuous assessment and evaluation of cybersecurity provides updated information about the ever-changing threat landscape, helping to protect genomic data and related assets over time. An effective cybersecurity program continually implements improvements, evaluating their effectiveness in safeguarding systems and sensitive data, such as genomic data.	2,5 - Assessments identify how well protections perform in safeguarding donors' and relatives' data, and provide input for continued effectiveness against updated threats and TTPs. 3 - Risk analysis is a point-in-time evaluation, so continuous assessment and evaluation is needed to provide a dynamic understanding of risk. 10 - Highly valued IP assets require ongoing protections and benefit from the continuous improvements identified through ongoing risk and controls evaluation. 12 - New technologies will be continuously assessed to identify needs for improvement.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	2	2	2	3	2	2	2	2	2	**1**	3	2	Organizations use security tests and exercises to maintain up-to-date risk models and determine opportunities or gaps where the organization can improve its risk response. Involving partners, suppliers, and third parties helps identify weaknesses in protections across the genomic data life cycle.	1 - Testing across the data life cycle discovers opportunities to improve protections to data quality and provenance, especially in data-sharing arrangements with third parties having different security postures. 7 - Testing exercises among partners and suppliers validate protections and promote trust between partners. 10 - Security test results can identify opportunities to improve the security posture of IP protections, including resilience and business continuity (for example, in the case of ransomware).
PR.PO-P8: Response and recovery plans are tested.	2	2	2	3	2	3	3	3	3	3	3	2	Testing plans ensures that plans remain effective and that changes to the operational environment have been appropriately addressed in the latest version. Testing provides confidence that an organization's planned approach is understood and communicated across stakeholders to achieve the desired outcomes, including minimizing inappropriate disclosure of genomic data and any further impacts.	2,5 - Testing plans ensures that response and recovery activities are effective to limit the privacy impact of an incident and recover to an acceptable state. 8,12 - When new technologies are introduced, there may be special needs for response and recovery to ensure that teams understand any new requirements. Additionally, testing helps ensure that response and recovery across partners are effective.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities.	2	2	2	3	2	2	3	2	2	2	3	2	Organizations incorporate lessons learned from operational reviews so that cybersecurity safeguards and protections for genomic data and related assets are maintained in a manner that is timely (for emerging threats) and effective (relevant for newly discovered vulnerabilities).	8 - Organizations conduct lessons-learned activities among research partners to identify gaps and attain minimum baseline protections that support reproducibility in research. 10 - Organizations improve IP protections, monitoring operations to identify security gaps and proactively fortify against future threats.
PR.PO-P5: Protection processes are improved.	3	3	3	3	3	3	3	3	3	3	3	2	As technology evolves and when new regulations are published, protection processes may need to be enhanced. Also, organizations will evaluate the implementation of newly available security or privacy features that are consistent with risk posture and risk strategy.	1 - Protection processes can include assurances that data are appropriate for processing purposes and that the chain of provenance remains intact. 2,4,5,8,12 - Specific PETs may require new processes to achieve the benefits, including data minimization, encryption, or de-identification.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PO-P6: Effectiveness of protection technologies is shared.	2	3	3	3	3	3	2	3	3	3	3	3	The genomic community will share the results of implementing protection strategies across research environments and other partners to manage the trust in data quality and provenance throughout the genomic data processing life cycle.	2,4,5,9 - Sharing across the ecosystem ensures that any issues impacting donors' or relatives' privacy are appropriately communicated in accordance with laws and policy. 6,8,12 - Researchers and technology providers will want to share any issues with data protections to ensure rapid remediation across the entire ecosystem and minimize the impact of unauthorized data access. 7 - Communication builds and maintains trust across partners.
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	2	2	**1**	3	2	2	**1**	2	2	**1**	3	2	Organizations use contingency plans (e.g., incident response, business continuity, disaster recovery) for responding to, recovering from, and learning from adverse events that can affect the operations of genomic processing and impact data quality, provenance, access, privacy, or consent, or negatively affect business continuity.	2,4,5 - Contingency plans include relevant information on processes for communicating with donors and relatives to inform them of privacy harms and adverse events (such as data breaches). 3 - Risk modeling identifies areas that require incident response activities to be included in the response plans. 7 - Maintaining contingency plans demonstrates due diligence and trustworthiness in managing cybersecurity risks. 10 - Plans will ensure that IP is protected when cybersecurity events occur, supporting the continuity of the organization's mission and viability.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	2	3	2	3	2	3	2	3	2	2	3	2	Managing risk within the genomic community includes being able to respond appropriately if a privacy event or breach occurs. When a privacy event or breach occurs with a system that has individuals' information, plans for responding and recovering systems and information will help minimize inappropriate disclosure of data, control any further impacts, and maintain trust and reputation.	2,4,5,9 - Response plans will include appropriate actions to identify, manage, and recover from privacy breaches, including notifying donors, returning to an acceptable state in accordance with consent agreements, and complying with legal and contractual requirements. 3 - Risk management strategies will include appropriate response planning and processes, including managing any adverse outcomes for the individuals affected. 7 - Response and recovery activities will directly impact an organization's reputation and the trust of partners who rely on the organization. 10 - Response and recovery plans identify any IP and associated activities to protect and recover it so that IP data is available to be used for business purposes.
PR.PO-P8: [Repeat]	2	2	2	3	2	3	3	3	3	3	3	2		

1246

Table 13 presents the CSF and cross-walked PF Subcategories for the Identity Management, Authentication, and Access Control (PR.AA) Category. The CSF description for this Category is: Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.

Table 13. Protect: Identity Management, Authentication, and Access Control (PR.AA).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	**1**	**1**	**1**	**1**	**1**	**1**	3	2	**1**	**1**	2	**1**	Managing identities and credentials enables other authentication and authorization capabilities for protecting genomic data.	1,6,10 - Robust identity and credential management enables an organization to manage access to genomic data throughout the life cycle and enforce accountability for data quality, provenance, and IP protections. 2,4,5 - Privacy protections require the ability to manage who accesses data and what they do with the data. This may be especially important for high-value data that can be used to link individuals. 8,12 - Shared environments and new technologies integrate identity and credential management to authenticate and authorize users, services, and assets.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**1**	3	2	2	2	**1**	2	**1**	2	**1**	3	**1**	Credentials manage access by defining who or what is authorized, specifying permitted actions, enabling access revocation when individuals depart, and binding access to credentials to ensure accountability and support incident response. This Subcategory will be prioritized in dynamic environments (e.g., researchers) with complex data-sharing interconnections to ensure that personnel are properly credentialed and the system boundaries and interconnections are properly monitored.	1,4,6 - Identity (of person, service, app, etc.) is used to monitor and manage data access to support data access, quality, provenance, and consent requirements. Consent travels with the data, with access managed at the identity level. 3,5 - Controlling access supports managing privacy risk by reducing exposure of data and the potential privacy harms due to genetic association/combining data sources that may result in data being identified/re-identified. 7,8,12 - Compromised identity will destroy trust, including trust between partners, even when using privacy-preserving technologies. Legacy and new technologies will both support consistent identity management.
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	2	3	2	3	3	2	3	3	3	2	3	2	Identity proofing provides a more granular level of access management that may not be applicable in all environments. As organizations implement a zero-trust architecture, they will want to assert authentication for high-risk data interactions.	1,3 - For high-value data, identity proofing enables organizations to implement more granular access controls in support of data quality and provenance. 6 - This capability will help organizations implement granular access control as part of a zero-trust architecture. 2,4,5,10 - These capabilities enhance sensitive data protections, aligned with

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														efforts to implement other requirements related to a zero-trust architecture.
PR.AC-P6: Individuals and devices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	2	3	2	2	2	**1**	2	2	2	2	3	2	Proofing and binding individuals and devices to credentials enable organizations to manage and understand who/what has access, verifying the actions individuals or devices are allowed to do, and implementing active controls for managing access and preventing unauthorized access. If a breach/event occurs, this can provide information on where unauthorized access might have come from.	1,6,8,9,10,12 - This level of granularity can be used to help manage data quality and provenance, research environment integrity, trust, reputation, legal and regulatory requirements, IP protection, and new technologies. 2,4,5 - Authentication commensurate with the risk of the transaction helps to implement additional privacy controls that protect consent based on the privacy risk.
PR.AA-03: Users, services, and hardware are authenticated.	**1**	**1**	2	2	**1**	**1**	3	**1**	2	**1**	3	**1**	Users, services, and devices accessing systems processing genomic data will authenticate using multifactor authentication with periodic re-authentication. Implementation will be aligned with other requirements related to a zero-trust architecture, including managing	1,2,4,5,10 - Authentication capabilities will be prioritized to enhance data quality, provenance, and access protections for privacy data and IP. 3,8,12 - Whenever data is shared or new technology is integrated, managing authentication, including remote access capabilities, helps control data access and reduce the risk of data corruption or loss.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													remote access, cloud, and highly collaborative environments.	
PR.AC-P3: Remote access is managed.	2	3	2	2	2	**1**	2	2	2	**1**	3	2	Remote access is the primary method used in genomic data environments and will be a priority across most MOs. Organizations will manage who has access (individuals or devices) and what they are allowed to do, revoking access when people leave. Ineffective remote access management may impact data quality, provenance, reputation and credibility, public perception, trust, compliance with legal and regulatory requirements, and the ability to protect IP.	1,9 - Some organizations may decide to manage remote access in a way that will prohibit local downloading of data (e.g., biobanks, commercial terms) to comply with legal /regulatory requirements around downloading. 2,4,5 - Remote access across partners will implement consistent, appropriate privacy protections according to consent requirements. 6,8 - All forms of remote access, including vendor updates and maintenance and access to research environments, will be managed. 12 - Technologies bring people to data via remote access. Authorized individuals need access to effective, controlled data-sharing capabilities. Adopting zero-trust principles remains relevant in this case, especially with the increased practice of using remote access [e.g., the 21st Century Cures Act allows remote access to personally identifiable information (PII) in research [20].]
PR.AC-P6: [Repeat]	2	3	2	2	2	**1**	2	2	2	2	3	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AA-04: Identity assertions are protected, conveyed, and verified.	2	2	3	3	2	**1**	2	2	3	2	3	2	Managing identity assertions for single sign-on and shared environments helps prevent unauthorized access.	1,3 - Verifying identity assertions can improve risk management and data protections by preventing unauthorized access. 2, 5, 6, 8, 10, 12 - Identity assertions support an organization's ability to manage access and prevent unauthorized access (e.g., by third parties, research partners, remote users).
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	**1**	**1**	2	2	**1**	**1**	2	2	2	**1**	3	**1**	Policies and procedures involved in managing access (e.g., least privilege, role-based access, separation of duties) protect against unauthorized or unwarranted access. Organizations limit access to only required parties and regularly review and update authorizations to ensure that only the people authorized to work with the data have access.	1,3,6,10 - These capabilities prevent issues with data quality, provenance, access, and sharing. 2,4,5 - Privacy protections rely on appropriate access management through least privilege, separation of duties, and role-based access control (or other more restrictive means) to manage who accesses data and what they do with the data. Access management not only protects the data but also enables privacy capabilities like processing requests made by individuals or partner organizations for amendment or deletion. 8 - Researchers and their partners proactively manage authorizations in environments where there is high turnover, fewer physical access controls, or a greater need to protect sensitive data.
PR.AC-P1: [Repeat]	**1**	3	2	2	2	**1**	2	**1**	2	**1**	3	**1**		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AC-P3: [Repeat]	2	3	2	2	2	**1**	2	2	2	**1**	3	2		
PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**1**	2	2	2	2	**1**	2	2	2	**1**	3	2	Least privilege and separation of duties support privacy objectives and requirements and will be enforced in all access control systems and across partners. Ineffective access permissions may impact data quality, provenance, reputation and credibility, public perception, trust, compliance with legal and regulatory requirements, and the ability to protect IP.	2,4,5 - Access controls determine who can do what with the data (via authentication and authorization), enabling consent management and protecting against loss or unauthorized access to donor or relative information. 3,8,9,10,12 - Risk assessment will evaluate and prioritize access controls to ensure privacy, protect IP, and comply with laws and regulations, particularly focusing on data-sharing partnerships.
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	3	2	3	3	2	2	3	2	3	2	3	2	Organizations protect the physical devices used for genomic data processing through physical access controls. Risks to sensitive data from physical access are common for certain locations (e.g., open campuses, high-traffic areas) and environments with labs, sequencers, and other equipment.	3,6 - Physical access risks are included in risk models along with access protections applying to physical environments. 8 - Organizations operating physical data-sharing environments may assign a higher priority to managing physical access.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AC-P2: Physical access to data and devices is managed.	2	3	3	3	3	2	2	2	3	2	3	3	Managing physical access is a basic security practice that will be prioritized based on the organization's perceived need to restrict physical access to the data due to sensitivity. High-traffic organizations with varied personnel and high transition rates (e.g., researchers, universities, hospitals) may decide to prioritize this for various reasons, including protecting genomic data. Physical access is revoked for individuals who change their roles or leave the organization.	1,6,8 - Physical access may not be the typical access vector, but organizations will manage who has physical access to data and devices to manage data quality and provenance across partners. Physical access to wet labs will also be managed. 10 - Access to IP will be managed consistent with any legal restrictions. Data owners and custodians will understand what they can access and how it can be used.
PR.PT-P3: Communications and control networks are protected.	2	3	3	3	3	3	3	3	3	3	3	3	Protecting communications and control networks includes managing risks of data leaks and unauthorized use while using solutions that can help with wider data sharing.	1,12 - This may be relevant to data storage and analysis needs within an organization or when using emerging technologies for transferring data. 8 - Protecting research networks may require technical security solutions that can help with wider data sharing with the research community.

Table 14 presents the CSF and cross-walked PF Subcategories for the Awareness and Training (PR.AT) Category. The CSF description for this Category is: The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.

Table 14. Protect: Awareness and Training (PR.AT).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	2	**1**	2	**1**	**1**	2	**1**	**1**	**1**	**1**	2	2	Instructing users how to actively participate in and be aware of security and privacy protections through training maximizes the impact of other security and privacy activities and reduces associated risks. Third parties require the same types of training and awareness of genomic data protection requirements. Ongoing training helps personnel understand the changing landscape regarding genomic-related laws and regulations and emerging threats (insider, phishing).	2,4,5 - Training includes privacy-related topics (e.g., personnel knowing what to do if they come across genomic data they shouldn't have access to). Training for suppliers and partners includes privacy requirements such as ensuring that consent travels with the data. 6 - Training helps enforce the same data access requirements across all parties. 7 - Organizations train users on how to manage reputational risks. 8,12 - Personnel in data-sharing environments are trained to understand their roles and responsibilities, including training on new technologies. 9 - Training helps maintain legal and regulatory compliance. 10 - Organizations with IP will ensure that those with access to IP understand how to protect it. 11 - Third parties who provide samples will understand the requirements for sample diversity.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.	**1**	2	2	2	2	**1**	2	**1**	2	2	2	2	The workforce will need specialized training in handling genomic data due to its unique characteristics and challenges that are present in the data life cycle, particularly the risks associated with the reach of data beyond any ecosystem participant, turnover of staff, or data diversity requirements. Policies are only effective if the workforce is trained on the value of the data, the risks of the environment, and the expectations for protections.	6 - Access controls among the various data roles (owners, stewards, users, custodians, processors) are generally recognized as a high priority, preventative technical control. 8 - Researchers need to manage the privacy protection issues introduced by high turnover in the workforce that is common in universities and other similar settings. 12 - Users from various organizations will have specialized training on technologies used by a research consortium.
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	2	**1**	2	2	**1**	2	2	**1**	**1**	2	2	2	Senior executive cybersecurity training equips them to make informed risk decisions, provide the resources for supporting capabilities, and set the culture for the organization. Privileged users (e.g., system administrators with elevated privileges who oversee data management permissions, conduct backups, and implement integrity-checking mechanisms) do not typically interact with genomic data in	2,4,5 - Specialized training equips personnel to recognize sensitive data and relevant privacy, legal, regulatory, and compliance constraints. 6 - Training helps implement the same data access requirements across all parties. 7,9 - Senior executives are the primary personnel responsible for managing risks to reputation and trust as well as legal compliance. 8,12 - In shared processing environments, personnel in specialized roles implement and ensure that

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													the way that system users do, but privileged users play an important role in ensuring that data protections are managed appropriately.	appropriate protections are in place, including personnel screening. Privileged users with access to shared data environments have a higher responsibility to protect the data and the environment. 10 - Senior executives and other privileged users are responsible for protecting IP. 11 - Third parties who provide samples understand requirements for sample diversity.
GV.AT-P2: Senior executives understand their roles and responsibilities.	2	3	2	2	2	2	2	2	**1**	2	2	3	Senior executives establish the governance policies, values, and priorities that will be used to set downstream practices for the day-to-day activities among staff. They are most accountable for legal requirements and assigning sufficient budget/resources to address privacy requirements.	2,4,5,7,8,11,12 - Leadership prioritizes awareness and training efforts and provides the resources to support implementation. Executives may also include Chief Privacy Officers. 9 - Senior executives will need to make a risk-based judgment call in cases where they cannot meet compliance obligations. They also need to be aware of local and international legal and regulatory compliance requirements.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.AT-P3: Privacy personnel understand their roles and responsibilities.	2	2	2	**1**	**1**	**1**	2	**1**	2	3	2	**1**	Privacy personnel act as primary advisors and subject matter experts in most situations for organizations handling human genomic data. They need to understand the legal, regulatory, personnel, and operating environment to manage the privacy expectations for the workforce whenever genomic data is processed, particularly when it is shared across external organizations to manage data quality, provenance, and access based on "need to know."	5 - Privacy personnel will align their priorities among the other mission-critical and operational priorities, since they are not always in a position to know and understand all details of mission and operations. 6 - Privacy professionals will integrate with security teams and advise on the implications of providing 'who' access to 'what', which will likely be based on predetermined rules. 8 - Research enterprises generally lack resources and expertise on privacy matters, so input from privacy professionals on many aspects of privacy will be required (e.g., HIPAA). 12 - The workforce will require training on the privacy implications of any new technology.
GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	2	2	2	2	2	**1**	2	**1**	2	2	2	2	Third-party data service providers and processors will be required to meet the same level of privacy protections as the original data owner, so they will need to understand what is required and will be subject to service level agreements to ensure protections are carried out. Any organization involved in data sharing will	4 - Consent will be consistently implemented across all organizations handling the data. 6,8,9,12 - Training and awareness will specify data-sharing requirements, how data access is managed, legal and regulatory requirements, and the risks from using newer technologies. 11 - Aligning to data diversity requirements among organizations with differing priorities will require a high degree of coordination.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													prioritize the consistent implementation of privacy requirements.	

Table 15 presents the CSF and cross-walked PF Subcategories for the Data Security (PR.DS) Category. The CSF description for this Category is: Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Table 15. Protect: Data Security (PR.DS).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	**1**	2	**1**	Data-at-rest protections are implemented whenever sensitive data is involved, including encryption and monitoring data access. Additional measures may be required to protect genomic data.	2,4,5,6,10 - Data protections, including encryption, prevent unauthorized access to sensitive data and can help prevent data leaks and data breaches. 7 - Lack of safeguards (or even the perception of the lack of such implemented safeguards) can impact trust and reputation. 8,12 - Data protections including encryption help manage sensitive data at rest for every partner. New technologies support future encryption and other protection technologies.
PR.DS-P1: Data-at-rest are protected.	**1**	2	**1**	2	**1**	2	2	2	2	**1**	3	2	Encrypting data-at-rest is one way of keeping data secure and is often a priority, though encrypting large files may result in additional costs.	1,6,10 - Encrypting data at rest protects stored data from unauthorized access, supporting data integrity and provenance, and protecting against leaks and breaches. 2,4,5 - Data-at-rest protections keep data secure but accessible by appropriate individuals in accordance with consent. 7,9 - Consistently applied practices such as encryption demonstrate that an organization can be trusted with data

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														and support compliance with legal and regulatory requirements and international standards for controlling access. 12 - Organizations ensure that new technologies support encryption requirements.
PR.DS-P5: Protections against data leaks are implemented.	2	**1**	2	2	**1**	**1**	2	2	2	**1**	3	2	Effective safeguards and protections will help manage access, protect against loss or disclosure, and reduce privacy risks to sensitive data, including IP. Data leaks may result in legal consequences, loss of reputation, and lack of trust in data quality or provenance.	2,3,4,5,7 - Organizations identify where privacy risks to donors and relatives might arise from data leaks and implement protections commensurate with their risk strategy to comply with consent requirements. 8 - Researchers ensure that all partners implement appropriate protections from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data. 12 - Organizations ensure that new technologies provide adequate protections against data leaks.
PR.DS-P6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	2	3	2	3	3	3	3	3	3	3	3	2	Integrity-checking mechanisms for software, firmware, and information help enforce the use of consistent data security practices, standards, and risk management tools.	1,6,12 - Integrity checking enforces consistent security practices that manage provenance, ensure data quality, and restrict access. These integrity-checking mechanisms are necessary for PETs testing and verification and could be helpful for emerging technologies.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PT-P1: Removable media is protected and its use restricted according to policy.	2	3	3	3	3	2	3	2	3	3	3	3	Removable media will be managed to reduce the likelihood of loss or theft of genomic data resulting in questions related to data provenance.	1,4,7 - When removable media is used, policies will help protect the media and the data's provenance, preventing data leaks and unauthorized use. 8 - Use of removable media introduces risks in protecting data when sharing among research partners. Enhanced or additional protections may be required as more researchers and partners gain access to genomic data. Organizations may need to limit use of removable media due to increased risk of loss and theft and because of other information beyond the genome.
PR.DS-02: The confidentiality, integrity, and availability of data in transit are protected	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	**1**	2	**1**	Data-in-transit protections are implemented whenever sensitive data is involved, including encryption and monitoring for data exfiltration or leaks. Additional measures may be required to protect genomic data.	2,4,5,6,10 - Data protections, including encryption, prevent unauthorized access to sensitive data and can help prevent data leaks and data breaches. 7 - Lack of safeguards (or even the perception of the lack of such implemented safeguards) can impact trust and reputation. 8,12 - Data protections, including encryption, help manage sensitive data in transit in data-sharing environments. New technologies support future encryption and other protection technologies.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.DS-P2: Data-in-transit are protected.	**1**	2	**1**	2	**1**	2	2	2	2	**1**	3	2	Encrypting large files may result in additional costs, particularly during transmission. Encrypting data in transit protects data from being intercepted, which can result in unauthorized access, data integrity and provenance issues, and data leaks and breaches.	2,4,5 - Encrypting data in transit keeps data secure but also accessible by appropriate individuals in accordance with consent. 7,9 - Consistently applied practices such as encryption demonstrate that an organization can be trusted with data and support compliance with legal and regulatory requirements and international standards for controlling access. 8 - As more researchers gain access to genomic data, enhanced or additional protections may be required, such as data-in-transit protections. 12 - Organizations ensure that new technologies support encryption requirements.
PR.DS-P5: [Repeat]	2	**1**	2	2	**1**	**1**	2	2	2	**1**	3	2		
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected.	**1**	**1**	2	**1**	**1**	**1**	2	**1**	2	**1**	3	**1**	Data-in-use protections are implemented whenever sensitive data is involved, including encryption and privacy-preserving technologies, which may require additional research to implement. Additional measures may be required to protect genomic data where a common approach	2,4,5,6,10 - Measures to prevent unauthorized access to sensitive data-in-use can help prevent data leaks and data breaches. 7 - Lack of safeguards (or even the perception of a lack of implemented safeguards) can impact trust and reputation. 8,12 - New technologies and cloud applications may facilitate data-in-use

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													is to write into temporary files, which will be protected and then deleted.	protections for researchers and their partners.
PR.DS-P5: [Repeat]	2	**1**	2	2	**1**	**1**	2	2	2	**1**	3	2		
PR.DS-11: Backups of data are created, protected, maintained, and tested.	**1**	2	2	2	2	3	3	2	2	**1**	2	2	Genomic data processing environments will consider multiple ways to back up the highly valuable genomic data due to size constraints. Access to backups will be restricted to prevent loss of sensitive data including IP and privacy data. Enterprise and system management plans consider both the roles and risks of backup management while preparing for ransomware or other outages.	1,10 - Backups enable recovery from an incident involving data quality issues or loss of sensitive data, including IP. This practice helps ensure provenance and manage data quality by providing a trusted state to restore to. 2,4,5 - Backups provide benefits but may also be an attack vector for sensitive privacy data. Backups will therefore include appropriate protections. 8 - Ransomware has become a primary threat for researchers. Genomic data continues to be a valuable target. Backups are the primary tool supporting data recovery.
PR.PO-P3: Backups of information are conducted, maintained, and tested.	2	3	2	3	3	3	3	3	3	2	3	2	Backups enable organizations to restore data to a trusted state after an issue occurs, if the validity of data is questioned, or if data becomes corrupt. Backups support managing the risks associated with data loss	1,8,10 - Backups directly impact the ability to have trusted data quality and provenance when there are issues involving the production data. Due to the value of genomic data, including IP, backups may serve to protect the investment in datasets despite the cost of storing such large datasets. Backups can reduce the time it takes to resume operations after an incident.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													(e.g., ransomware) and are considered a best practice.	12 - Whenever new technologies are introduced, the risk becomes higher for data issues, and backups may be considered a higher priority.

Table 16 presents the CSF and cross-walked PF Subcategories for the Platform Security (PR.PS) Category. The CSF description for this Category is: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.

Table 16. Protect: Platform Security (PR.PS).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PS-01: Configuration management practices are established and applied.	**1**	2	2	2	2	2	3	3	2	**1**	3	2	Configuration management practices implementing secure baseline configurations manage risks from vulnerabilities in IT, operational technology, or industrial control systems, including genomic sequencers. Baseline configurations facilitate building systems that are secure to start, maintain secure configurations (e.g., patching), and detect anomalous behavior in response to threats or incidents. They manage risk by significantly reducing the likelihood and impact of unauthorized access or making unauthorized changes to the data or environment.	1,3,6,10 - Configuration management practices reduce the attack surface by minimizing vulnerabilities that may result in issues with data quality, provenance, data access, susceptibility to removable media attacks, and exposed IP. 2,4,5 - Configuration management processes ensure that systems and environments maintain privacy-related cybersecurity capabilities as changes occur over time and that privacy protections (e.g., minimization, consent) remain in place throughout such changes. 8,12 - Data-sharing environments implement effective configuration management control to protect data, analyses, and results, managing risks for sensitive information (e.g., stolen data or misuse) by ensuring authorized access to research results. Technology solutions will include recommended secure configurations.
PR.PT-P1: [Repeat]	2	3	3	3	3	2	3	2	3	3	3	3		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	**1**	3	2	**1**	2	**1**	3	3	3	2	3	2	Least functionality supports achieving privacy minimization. Least functionality can help when there are no existing technologies that manage access and prevent surprises in data processing. Overall, least functionality helps reduce the likelihood of breaches, helps properly secure and safeguard genomic data, and can impact data quality, provenance, trust, reputation, protection of IP, and the integrity and availability of research environments.	4,5 - Least functionality helps reduce risks to data exposure and associated privacy risks. 6,12 - Least functionality ensures access is limited to the minimum necessary and restricted to only the data required, particularly when sharing or coordinating across multiple organizations. Least functionality will have the highest degree of protection and will be enforced on all new technologies.
PR.PO-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	**1**	2	2	2	2	2	3	3	**1**	2	3	**1**	Standardized configuration baseline management reduces the attack surface exposed by misconfigurations to maintain data processing consistency with appropriate protective mechanisms and security principles, including least functionality. Baselines support monitoring for changes (expected and unexpected) to identify	1 - Baselines ensure an understanding of the expected environment when monitoring for changes or issues with data processing and quality. 3,4 - Configurations will be used to optimize protective technologies to reduce privacy risk and align with consent. 12 - New technologies will incorporate configuration management baselines to ensure least functionality and ensure the platform, device, or software doesn’t

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													anomalies and respond appropriately, contributing directly to data quality and provenance, protecting against unauthorized access, and supporting legal protections.	introduce additional privacy or security risks.
PR.PO-P2: [Repeat]	**1**	3	2	3	2	2	3	3	3	3	3	**1**		
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	2	2	2	2	2	2	3	2	3	2	3	2	Organizations are responsible for comprehensive management of software in their environment, including addressing any vulnerabilities through scanning, remediation, disclosure, and countermeasures to protect sensitive privacy data or IP. Proper maintenance, including patching, removing unauthorized software, and replacing end-of-life software, helps address vulnerabilities that could impact the security of genomic data or data processing environments.	1,3,6,7 - Proper software maintenance throughout its life cycle mitigates vulnerabilities and helps maintain data quality and provenance. Effective software management includes processes for approving the use of open-source software, monitoring remote access, implementing patches, and vulnerability management. 2,4,5 - Some software vulnerabilities may introduce privacy risks that lead to problems for individuals (e.g., discrimination, loss of autonomy, loss of trust) and related risks for the organizations (e.g., compliance, reputation). 9 - Laws or guidance may stipulate migration away from unsupported software. Federal organizations follow legal and regulatory requirements for vulnerability management programs,

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														including time to mitigate high or critical vulnerabilities [21].
PR.DS-P3: [Repeat]	**1**	2	2	3	**1**	2	3	3	2	2	3	2		
PR.DS-P6: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	2		
PR.MA-P2: [Repeat]	2	3	3	3	3	2	3	3	3	2	3	3		
PR.PO-P10: [Repeat]	2	3	**1**	3	3	3	3	3	3	3	3	2		
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	2	3	3	3	3	2	3	2	3	2	3	2	Genomic processing organizations, including academic and research environments, may contain unsupported or outdated hardware, whose use introduces vulnerabilities and risks to sensitive data. Prior to hardware disposal, any sensitive data will be erased (e.g., purged, cleared, wiped) to prevent unauthorized access or unauthorized attempts to recover sensitive data.	1,8,10 - Improper use or disposal of unsupported or outdated hardware introduces risks that may threaten data quality, provenance, and access to sensitive data including IP. 2,4,5 - Managing data on assets, particularly through the disposition process, supports the implementation of privacy requirements, which often include data retention and disposition constraints. 9 - Laws or guidance may stipulate migration away from unsupported hardware. 12 - The hardware used in technology solutions may become outdated and will be replaced following hardware disposal processes to prevent exposing sensitive data.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.DS-P3: [Repeat]	**1**	2	2	3	**1**	2	3	3	2	2	3	2		
PR.DS-P8: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	3		
PR.MA-P1: [Repeat]	2	3	3	3	3	3	3	3	3	2	3	3		
PR.PS-04: Log records are generated and made available for continuous monitoring.	**1**	2	**1**	2	2	2	3	2	**1**	**1**	3	2	Log records assist in auditing activities and accountability by identifying who, what, and when changes to data or the environment occurred. The logs may indicate issues with data quality, provenance, unauthorized access, or data transfer. This practice supports incident response investigations that identify misuse and determine what happened and who is responsible. Logs track remote access, including remote maintenance.	1,3,6,8,10,12 - Generating log records helps manage data quality, provenance, and data access. Logs facilitate accountability in the event of unauthorized or malicious activity. All devices and software will be monitored and support logging. 2,4,5 - Log records may help detect and understand privacy events related to data quality, changes, unauthorized access, or disclosure. 6,8,12 - Organizations with remote maintenance of shared and cloud environments will take extra precautions to implement effective access controls, such as generating log records, that support event correlation to detect malicious behavior. 9 - Log records verify compliance, identify noncompliance, and support legal discovery.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**1**	2	2	2	2	**1**	3	2	**1**	2	3	**1**	Audit records help track and manage data quality, provenance, access, sharing, and changes while supporting risk management measures and compliance with consent, laws, and regulations. They help maintain the data provenance required for confidence in datasets for research and data sharing across large communities.	2,4,5,7 - Audit records can help identify data exposure, unauthorized access, or the extent of a data breach to determine who needs to be notified and whether consent was managed appropriately. Logs help monitor data access to prevent hoarding of donor data and making unwanted changes, as well as to manage changes to individuals' preferences and consent. Data marked for deletion that has not been deleted may be identified. 12 - New technologies support audit logging to be accountable for whatever happens with the data.
PR.PS-05: Installation and execution of unauthorized software are prevented.	**1**	3	2	2	2	**1**	2	**1**	2	**1**	2	**1**	Organizations will implement capabilities to detect and prevent the installation of unauthorized software, alongside monitoring for unauthorized users, connections, devices, and network or personnel activity. Organizations detect suspicious events by using allow-lists and deny-lists to inform the security tools that log and audit system activity. Organizations will "lock down" their systems so that only authorized	1,3,6,8,10 - Providers, research environments, and those with IP use these capabilities to prevent inadvertently sharing malicious software with partners that may compromise sensitive data. 12 - New technologies support software asset management by identifying all software used by the technology through an SBOM, interoperability with software monitoring, and proper logging of all software activity.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													personnel can install authorized software.	
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle.	**1**	2	2	2	2	2	3	3	2	**1**	3	2	A software development life cycle provides a framework to manage software security through all life cycle phases (e.g., development through operations).	1,6, 8,10,12 - Secure software and system development life cycle principles implement and manage controls for systems throughout the genomic data life cycle that reduce the risk of issues with data quality, provenance, access, IP protection, and new technologies. 2,4,5 - The secure software development life cycle includes processes and activities that address the privacy risks associated with processing genomic data (e.g., privacy engineering practices).
CT.PO-P4: [Repeat]	**1**	2	2	2	2	2	3	3	2	3	3	**1**		

Table 17 presents the CSF and cross-walked PF Subcategories for the Technology Infrastructure Resilience (PR.IR) Category. The CSF description for this Category is: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

Table 17. Protect: Technology Infrastructure Resilience (PR.IR).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	2	**1**	2	2	**1**	**1**	3	**1**	2	**1**	2	**1**	Organizations protect their network traffic from potentially malicious attacks by using technologies such as boundary protections, segmentation, firewalls, remote/logical access controls, or not permitting the processing of sensitive data in non-production environments. These protections limit unwarranted access, exposure, and manipulation of sensitive genomic data when sharing internal or external to the network.	2,4,5,10 - These controls help protect sensitive data, including privacy data and IP. 3 - Risk models identify ways to mitigate the risks of using cloud environments or other environments with remote access. Network access and integrity tools help manage these security risks. 8,12 - Organizations operating collaborative data-sharing environments prevent data from being exposed or altered by implementing remote and logical access controls consistently, using network integrity controls, and restricting use of sensitive data in non-production environments.
PR.PT-P3: [Repeat]	2	3	3	3	3	3	3	3	3	3	3	3		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.DS-P7: The development and testing environment(s) are separate from the production environment.	2	3	3	3	3	2	3	3	3	3	3	3	Separate development and testing environments may be prioritized for developing new systems and technologies, particularly when using cloud services.	3 - Risk assessments will identify potential risks for cloud-based processing in development and testing environments, which will generally be protected like a production environment. Highly sensitive data may exist in criminal justice, healthcare, and clinical lab environments. 4 - Organizations will be cautious with risks associated with AI model development and consent. While typically not taking operational action based on processing in development and testing environments, data security best practices will be used to ensure data privacy by protecting against leaks and breaches. Protecting non-production environments reduces the risk of genomic data being used without consent.
PR.AC-P3: [Repeat]	2	3	2	2	2	**1**	2	2	2	**1**	3	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	2	3	3	3	3	2	3	3	3	2	3	2	Segmentation is a best practice that will be prioritized by organizations to keep sensitive information (e.g., IP, patient/donor information) in protected areas only and in conjunction with other practices including zero trust principles. Segmentation helps prevent escalation of privileges, providing a level of support against insider threat.	1 - Segmentation supports minimizing uncontrolled or unauthorized access that impacts data quality. 3,12 - Segmentation is a component of remote access and zero trust. 6 - Segmentation prevents unauthorized access and manages authorized access. Control of network segments supports access controls to help prevent privilege escalation. 10 - Organizations may keep information regarding IP in a separate network segment.
PR.IR-02: The organization's technology assets are protected from environmental threats.	2	2	2	2	2	2	3	3	2	2	2	2	Organizations assess environmental threats to determine if the physical location is likely to experience impact from flooding, fire, wind, heat, or humidity. Genomic data processing environments may include devices (such as sequencers) that are expensive and warrant additional protections.	3 - Organizations consider known environmental threats (e.g., wildfire, flooding, excessive heat or humidity) where organizational equipment may be located or housed. 8,10,11,12 - Shared data processing environments will incorporate protections for locally stored data and meet legal requirements (e.g., Clinical Laboratory Improvement Amendments).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	3	3	3	2	3	3	3	3	2	3	3	3	The physical operating environment may not be prioritized as highly since data is frequently exposed through virtual access. When organizations process data on-premises, data protections for that environment will be prioritized. This may be particularly challenging for hospitals, research institutions with multiple partners, and universities with significant turnover.	3,8,12 - Organizations will want to manage risks to sequencers and other equipment, including new technologies.
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	3	3	3	3	3	3	3	3	3	3	2	Protections to maintain resilience will be a higher priority for operations requiring a high degree of availability (e.g., for research, healthcare), uptime, or business process continuity.	1,3,8 - Availability, as ensured by resilience mechanisms, is important for MOs where information or research is being shared across a supply chain. 9 - Certain sectors may have laws or regulations that stipulate uptime requirements that would require resilience mechanisms. 10 - Organizations protecting IP may prioritize resilience higher, potentially in cases where the use of the IP is tied to outcomes that may be potentially impacted by outages. 12 - New technologies will be selected to meet organizational resilience requirements.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	3	3	3	3	3	3	3	3	3	3	3	2	Use of these safeguarding protective mechanisms is dependent on the stage in the data processing pipeline. They may be most helpful with emerging technologies.	8,12 - Resiliency mechanisms may be prioritized in certain environments (e.g., hospitals) and can help with the availability of data sharing with the research community.
PR.IR-04: Adequate resource capacity to ensure availability is maintained.	3	3	3	3	3	3	3	3	3	2	3	2	Organizations with higher availability requirements manage capacity to ensure they can meet those requirements.	8,10 - Capacity and availability will be a higher priority in data-sharing environments, particularly if they are for time-sensitive applications such as healthcare.
PR.DS-P4: Adequate capacity to ensure availability is maintained.	2	3	3	3	3	3	3	2	3	3	3	2	Capacity requirements will be prioritized in contexts where availability matters, such as support service providers, law enforcement, research environments, and PET processing.	2,5 - Capacity can directly impact individuals when decisions are being made about them based on their data. 6 - Adequate availability reduces the need to download genomic data. 12 - Organizations will ensure that new technologies support data availability requirements.

Table 18 presents the CSF and cross-walked PF Subcategories for the Continuous Monitoring (DE.CM) Category. The CSF description for this Category is: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

Table 18. Detect: Continuous Monitoring (DE.CM).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.CM-01: Networks and network services are monitored to find potentially adverse events.	2	3	3	3	3	**1**	3	2	2	2	3	2	Organizations continuously monitor networks and interconnected systems for malicious code and unauthorized changes, as well as users, connections, devices, tools, access, and software. Monitoring ensures that systems function the way they were intended for a secure environment. Organizations can use allow-lists and deny-lists to inform security tools that log and audit system activity to support monitoring activities and detect suspicious events.	1 - Organizations monitor for data quality and provenance issues throughout the life cycle. 2,4,5 - Monitoring will detect when privacy data has been accessed inappropriately. 6,8,10,12 - Network monitoring helps protect data (e.g., IP, new technology) and sensitive research from events such as unauthorized access or ransomware. 9 - Monitoring supports legal discovery.
DE.CM-02: The physical environment is monitored to find potentially adverse events.	3	3	3	3	3	**1**	3	3	3	2	3	3	Although the likelihood of a physical attack vector may be lower, organizations monitor to detect and log physical access for control of sensitive data including research data, privacy, and IP.	6 - Organizations monitor the physical environment for unauthorized access, including to physical assets or genomic data processing components. Threat modeling has demonstrated that physical environments can be a significant area of risk. 10 - Monitoring physical access to any facilities where IP is stored supports incident investigations.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.	**1**	3	2	2	2	**1**	2	**1**	2	**1**	2	**1**	Monitoring personnel activity enables organizations to conduct privacy incident detection (including potential insider threats) and identify unauthorized changes or access that could impact the data, its validity, and its uses.	1,2,4,5,6,10 - Personnel access to sensitive data (e.g., privacy data, IP) will be restricted and monitored to detect activity (e.g., unauthorized access) that could compromise data and its integrity or provenance. 8,12 - Managing personnel activity will be prioritized in environments that share space and physical access, such as research or academic environments.
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events.	**1**	3	2	2	2	**1**	2	**1**	2	**1**	2	**1**	The genomic data processing environment involves multiple partners relying on each other to share data and services, broadening the attack surface. Monitoring external service providers ensures that data security requirements are met for data quality, provenance, access, and other protections across the data life cycle. Requirements for external providers' and the internal organization's data processing will be the same. The cost of active monitoring will be weighed against the benefits. Many laws and regulations, as well as federal compliance programs, require monitoring.	1,6,8 - All parties in data-sharing environments will have detection processes in place to consistently protect data quality throughout the life cycle. Monitoring will be consistent across external service providers through the implementation of the same or comparable access controls and the willingness to share monitoring alerts. 10 - Sensitive data may be targeted by external providers; organizations detect unauthorized attempts to access sensitive data such as IP. 12 - Organizations monitor new technologies to ensure they are functioning as designed.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	2	2	2	2	2	**1**	3	2	2	2	2	2	Monitoring hardware, software, environments, and data helps identify potentially adverse events that may impact operations or the genomic data itself. Genomic data processing organizations rely on an interconnected ecosystem that handles sensitive data and produces high-value results. Monitoring helps identify when an adverse event may indicate issues with data quality, provenance, access, etc.	2,4,5 - Privacy-related attacks can occur due to integrity issues (e.g., data leaks, malicious code, unauthorized code) with hardware and software. 6,8,10,12 - This monitoring identifies events that may indicate unauthorized access or malicious software that affects the quality of research, IP, or other results. 12 - New technologies may introduce hardware, software, or other data that may disrupt other assets and impact outcomes.
PR.DS-P6: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	2		
PR.DS-P8: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	3		

Table 19 presents the CSF and cross-walked PF Subcategories for the Adverse Event Analysis (DE.AE) Category. The CSF description for this Category is: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

Table 19. Detect: Adverse Event Analysis (DE.AE).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.	**1**	3	2	3	2	**1**	3	**1**	2	**1**	3	2	The Respond Subcategories rely on effective detection and analysis to determine the appropriate response activities. Analysis teams will understand the intricacies and potential threats to genomic data to better understand the impact of any events.	**1** - Analysis will determine if the attack impacted data quality or provenance. 2,4,5 - Analysis will determine if the attack involves privacy or consent issues. 6,10 - The analysis may determine if the attack exposes sensitive data, including unauthorized access or threats to IP.
DE.AE-03: Information is correlated from multiple sources.	2	3	3	3	3	2	3	2	3	2	3	2	Correlation helps provide a broader understanding of potential attacks across the organization to help identify similar attacks across different systems. Correlation requires additional resources and expertise and is sometimes considered a more mature activity.	**1**,3,6,8,10 - Correlation facilitates the ability to hunt for similar attacks across the network that may impact data quality, provenance, access, IP, research results, or the data life cycle. 2,4,5 - Correlation can help to coordinate the response to attacks that result in privacy impacts.
DE.AE-04: The estimated impact and scope of adverse events are understood.	**1**	3	2	2	2	**1**	2	**1**	2	**1**	3	2	Impact analysis will help determine if assets or data involved in a response effort include a privacy breach or issues with consent, data quality, provenance, or IP.	**1**,6,8,10 - Analysis teams will want to understand the nuances of genomic data processing to determine the impact and appropriate response to issues with data quality, provenance, access, research, and IP.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.AE-06: Information on adverse events is provided to authorized staff and tools.	2	3	2	2	2	2	3	3	2	2	3	2	Initial communication of event detection triggers response activities and informs appropriate parties of potential unauthorized access, privacy breaches, and compromised IP so they can determine appropriate response activities.	2,4,5,6,10 - Organizations processing sensitive data, such as data that impacts privacy and IP, will prioritize detection communication processes higher and ensure that authorized staff are appropriately identified in response plans.
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis.	2	3	2	3	3	2	3	2	3	2	3	2	Cyber threat intelligence (CTI) identifies potential attackers who may be interested in genomic data. Information sharing and analysis centers (ISACs) such as the Health-ISAC or the BIO-ISAC provide CTI that may alert organizations of similar attacks and the TTPs used. This information can help analysis teams identify and respond to adversarial threats and attacks more effectively.	1,3,6,8,10 - CTI and related context improve the ability to identify similar attacks across the network that may impact data quality or provenance, or be targeted at research organizations or specific IP. 2,4,5 - CTI and related context may indicate that specific adversaries are using specific TTPs targeted at human genomic data.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.	2	3	2	2	2	2	3	**1**	2	2	3	2	When an organization declares an incident, it activates related response teams including communications, forensics, and privacy incident response teams.	2,4,5 - Incident criteria include indicators for identifying incidents that have or may impact privacy and that require coordination with the privacy incident response team to determine whether additional privacy response activities are necessary. 6,8,10 - An incident involving data access, research data, or IP will have specific response requirements that include notification of specific teams and response activities. 7 - Thresholds may indicate the need to involve public relations teams if there is a risk to reputation.

Table 20 presents the CSF and cross-walked PF Subcategories for the Incident Management (RS.MA) Category. The CSF description for this Category is: Responses to detected cybersecurity incidents are managed.

Table 20. Respond: Incident Management (RS.MA).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	1	1	1	2	1	1	1	1	1	1	2	1	Executing the incident response plan in coordination with relevant third parties ensures a comprehensive and efficient response to incidents across all parties involved. This coordination helps mitigate the impact on sensitive data and facilitate recovery.	1,6,8,12 - Response operations manage any impact on data quality and provenance, quickly mitigate any unauthorized access, coordinate across all partners, and address any issues with new technologies. 2,4,5,9 - Organizations execute the incident response plan to manage the impact of privacy breaches in compliance with laws and regulations, communicating the impact on donors and relatives as required. 3 - Executing the response plan puts into practice the risk management activities identified through risk modeling.
RS.MA-02: Incident reports are triaged and validated.	1	1	2	2	1	1	2	3	2	1	2	2	Triaging and validating incident reports prioritizes response operations based on accurate information, ensuring communication with identified parties, and allocating appropriate resources for investigations to determine if, how, and to what extent human genomic data has been impacted.	1,6 - Appropriate response helps manage the impact on data quality, provenance, or access. 2,4,5 - Triage processes help organizations determine the extent of a compromise and whether it affects a donor, donor's relatives, or both, informing genomic data breach responses. 10 - Organizations with IP will want to quickly diagnose any impact on the IP and manage the response appropriately.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.MA-03: Incidents are categorized and prioritized.	**1**	**1**	2	2	**1**	**1**	2	3	2	2	2	2	Categorizing and prioritizing incidents helps allocate resources effectively to focus attention on the most critical incidents to minimize impact.	1,6,8 - Incidents that impact data quality, provenance, or access are categorized and prioritized to expedite remediation and restore confidence in the data for research or other purposes. 2,4,5,10 - Categorizing ensures that IP and privacy-related incidents are handled with appropriate urgency.
RS.MA-04: Incidents are escalated or elevated as needed.	2	2	3	2	2	2	2	2	2	2	3	2	Escalating or elevating incidents as needed ensures that the appropriate level of attention and resources are allocated to incident response to minimize the impact on genomic data, address legal cybersecurity or privacy requirements, and restore operations quickly.	1,6,8 - Incidents that impact data quality, provenance, or access (whether unauthorized access by authorized users or access by unauthorized users) are escalated to apply appropriate resources to the incident response and recovery. 2,4,5,10 - Escalation ensures that IP or privacy-related incidents are handled with appropriate urgency.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.MA-05: The criteria for initiating incident recovery are applied.	**1**	2	2	2	2	2	**1**	2	2	**1**	2	2	Applying criteria for initiating incident recovery ensures that the organization and related partners can systematically address and recover from incidents, minimizing the impact and expediting recovery to normal operations. Recovery plans identify applicable requirements from laws, policies, consents, and regulations and criteria for resuming operations and assessing impacts to privacy.	1,6,10 - Incidents that impact data quality, provenance, access, or IP are evaluated against pre-defined criteria to apply appropriate resources to the incident recovery and coordinate across all partners. 2,4,5 - Applying pre-defined criteria supports an organization's ability to determine if recovery operations (e.g., escalations, notifications) need to be initiated in response to a privacy or consent-related incident.

Table 21 presents the CSF and cross-walked PF Subcategories for the Incident Analysis (RS.AN) Category. The CSF description for this Category is: Investigations are conducted to ensure effective response and support forensics and recovery activities.

Table 21. Respond: Incident Analysis (RS.AN).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	2	2	2	2	2	**1**	3	3	2	2	2	2	Effective analysis of incidents involving genomic data establishes an understanding of what happened, the impact, and root causes. Organizations use this analysis to minimize the likelihood of similar incidents by refining security measures and improving incident response strategies, enabling effective mitigation of risks.	1,6,10 - This analysis helps prevent further incidents, addressing the impact on data quality, provenance, IP, and access. 2,4,5 - Performing analysis, including forensics if needed, determines whether consent agreements were violated and the resulting impact on donors or their relatives. 9 - Establishing what has taken place and the root cause may help identify any legal or regulatory reporting requirements.
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	2	2	2	2	2	**1**	3	3	2	2	2	2	Recording actions performed during an investigation and preserving the records' integrity and provenance documents the organization's comprehensive compliance with procedures, as well as legal and investigation requirements. This helps the organization maintain accountability and transparency, manage trust and reputational issues, and respond to legal or regulatory actions.	1,6 - Records can be used to enforce accountability of actions (e.g., access) during an incident and promote transparency of the investigative actions to support the preservation of quality and trustworthy genomic data throughout its life cycle. 3 - Documenting all investigative actions helps identify, model, and mitigate cybersecurity and privacy risks in the processing of genomic data.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	3	2	3	3	2	2	3	3	2	2	3	2	Managing the incident data and metadata supports the overall incident management life cycle, ensures accurate reporting, and helps prevent future similar incidents.	1 - Proper handling of incident data helps document any issues with data quality and provenance. 2,4,5,6 - Incident data and metadata support investigations that inform privacy impact and an incident's magnitude, allowing for a thorough understanding of how incidents occurred. The data helps document access to sensitive data and ensures that access is managed to prevent corruption or deletion and minimize the likelihood of future incidents. 7,9 - Records may be needed for legal purposes and can be used to demonstrate the vigilance needed to repair reputational issues.
PR.DS-P6: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	2		
RS.AN-08: An incident's magnitude is estimated and validated.	**1**	**1**	2	2	**1**	**1**	2	3	2	**1**	2	2	Understanding an incident's magnitude enables organizations to respond to an incident proportional to its impact, gaining insights into the actual impact of an incident as it occurs.	1,6,10,11 - This assessment helps quantify the full impact on data quality, provenance, IP, and access and may help assess any impact on sample diversity. 2,4,5 - When privacy data is involved, the magnitude of the incident helps determine the specific reporting requirements and activities needed to prevent further issues.

Table 22 presents the CSF and cross-walked PF Subcategories for the Incident Response Reporting and Communication (RS.CO) Category. The CSF description for this Category is: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.

Table 22. Respond: Incident Response Reporting and Communication (RS.CO).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.CO-02: Internal and external stakeholders are notified of incidents.	2	2	2	1	2	2	2	1	1	2	2	2	Notifying stakeholders (e.g., donors, research partners, suppliers) about incidents supports transparency so all parties can take necessary actions to mitigate potential risks. Effective communication of incidents manages the immediate and long-term impacts on the organization and its stakeholders and starts the process of restoring trust in the data and the organization.	1,8 - Any impact on data quality or provenance is communicated to stakeholders and partners who share the data or results from processing the genomic data. 2,4,5 - Consent is managed across the data life cycle, and issues with consent require taking action, including notification. A privacy breach requires the organization to notify donors and inform them of any issues with consent. Public notification of the breach may be the only way to help relatives identify that there may be an issue with their data. 9 - Notification is required legally for certain types of incidents, such as privacy breaches. 11 - Communicating incidents that affect sample diversity helps affected populations understand any potential impact on sample diversity.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.CO-03: Information is shared with designated internal and external stakeholders.	2	2	2	2	2	2	2	2	2	2	2	2	Sharing information about incidents with designated stakeholders coordinates response and recovery efforts, facilitates the sharing of threat intelligence about observed TTPs, alerts senior leadership of incident status and impact, and coordinates with partners who share the data. Laws, regulations, and contracts will stipulate information-sharing requirements.	1,8 - Communication promotes repairing any issues with trusting data provenance and integrity as needed for research partners. 2,4,5 - Coordination with designated stakeholders helps manage privacy response and recovery activities. 6 - Communicating how TTPs resulted in unauthorized access can help stakeholders improve their defenses against similar attacks.

Table 23 presents the CSF and cross-walked PF Subcategories for the Incident Mitigation (RS.MI) Category. The CSF description for this Category is: Activities are performed to prevent expansion of an event and mitigate its effects.

Table 23. Respond: Incident Mitigation (RS.MI).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RS.MI-01: Incidents are contained.	1	1	2	2	1	1	3	3	2	1	3	1	Containing incidents is the first step in mitigating their impact. This process involves immediate actions to prevent the incident from spreading and causing further damage.	1,6 - Containment prevents further impact on data quality and provenance while minimizing unauthorized access to data. 2,4,5 - Containment limits the impact of privacy-related incidents. 8,10,12 - Containment helps limit the impact on IP across research partners and from technology solutions.
RS.MI-02: Incidents are eradicated.	1	1	2	2	1	1	3	3	2	1	3	2	Eradicating incidents involves removing the root cause to eliminate any impact from the threat, enabling transition to recovery operations, and preventing recurrence.	1,6 - Eradication prevents further impact on data quality and provenance and minimizes the potential for additional unauthorized access to data. 2,4,5 - Eradication helps prevent further impact of privacy-related incidents. 8,12 - Eradication helps stop the impact on IP across research partners and from technology solutions.

Table 24 presents the CSF and cross-walked PF Subcategories for the Incident Recovery Plan Execution (RC.RP) Category. The CSF description for this Category is: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

Table 24. Recover: Incident Recovery Plan Execution (RC.RP).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	**1**	2	2	2	2	2	**1**	2	2	**1**	2	2	Recovery plans help restore data access and quality to an acceptable operational state and communicate recovery status across partners. Having an effective recovery plan helps manage risk across partners who rely on trusted operations, impacts to IP and privacy, and applicable requirements from laws, policies, consents, and regulations.	1,8,11,12 - Recovery plan activities coordinate across partners to track progress toward being able to trust the data and return to normal operations. Involving all partners and technology solutions helps ensure comprehensive recovery. 2,4,5,9 - Recovery activities address legal, policy, regulatory, privacy, and consent requirements. 3,10 - The recovery plan manages high-risk recovery operations and impacts to IP. Risk modeling and tolerances may help determine the scope and resourcing required to manage recovery operations. 6 - Recovery plans incorporate and enforce data access protection requirements, including access control for backups. 7 - Recovery plans include communications required to maintain and restore trust in the organization.
PR.PO-P7: [Repeat]	2	3	2	3	2	3	2	3	2	2	3	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	**1**	2	2	2	2	2	**1**	2	2	**1**	2	2	Determining which recovery actions to prioritize and perform helps organizations have data quality and other protections in place prior to resuming normal operations in a trusted, uncompromised state.	1,10 - Prioritized recovery actions include those that restore data quality, protect provenance, and protect IP. 2,4,5,9 - Prioritize recovery actions that address legal, policy, regulatory, privacy, and consent requirements. 7 - Prioritized recovery actions include those that maintain and restore the trust in and reputation of the organization.
PR.PO-P8: [Repeat]	2	2	2	3	2	3	3	3	3	3	3	2		
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.	**1**	2	2	2	2	3	3	3	2	2	2	2	Managing backups is a basic function that can prevent data loss and protect against ransomware. Confirming backup integrity verifies a trustworthy state prior to using or sharing the data.	1,10 - Backups enable recovery from an incident involving data quality issues or loss of sensitive data, including IP. Verifying integrity identifies any data tampering that may impact data quality, provenance, or compromise. 2,4,5 - Backups provide benefits but may also be an attack vector for privacy data. Enterprise and system management plans consider both the roles and risks of backup management, including checks to verify privacy data quality.
PR.PO-P3: [Repeat]	2	3	2	3	3	3	3	3	3	2	3	2		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms.	2	3	2	2	3	2	3	2	3	3	3	2	Considering critical mission functions and recovery of cybersecurity risk management functions helps verify a return to a trustworthy operational state. Organizations processing genomic data tend to be sharing with data partners, resulting in a complex ecosystem required to produce the outcome, whether it be research, IP, or law investigation, and they depend on knowing when the data and environment are trustworthy again.	8 - Research-heavy organizations will want to know when restoration of systems has occurred and whether the data used in research is available and of trustworthy quality. 12 - When new technologies are impacted by an incident, post-incident activities ensure that any vulnerabilities have been addressed and that new post-operational norms include implementing additional or new cybersecurity risk management activities moving forward.
ID.BE-P2: [Repeat]	3	3	2	3	3	3	2	2	2	2	2	3		
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	**1**	2	2	2	2	2	2	2	3	2	2	2	Any compromised asset may introduce vulnerabilities and risks to data quality, provenance, access controls, IP protections, and integrity of new technologies. After verifying asset integrity, organizations will confirm the integrity of the genomic data pipeline and a return to normal operating status.	8 - Researchers will want to verify that both they and their suppliers and partners have fully checked asset integrity to confirm recovery status. 12 - When new technologies are impacted by an incident, Recover activities ensure that any asset integrity issues have been addressed.
PR.DS-P8: [Repeat]	2	3	2	3	3	3	3	3	3	3	3	3		

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed.	2	3	3	3	3	3	3	3	3	3	3	3	At the end of an incident, communication across genomic data processing partners helps confirm full operational status and a trustworthy genomic data pipeline.	1,3,6,10,12 - Documenting and resolving incident-related lessons learned will help reduce the likelihood of future incidents. 2,5 - Post-incident recovery activities will include confirmation that any incidents involving privacy-related breaches have been addressed.
PR.PO-P7: [Repeat]	2	3	2	3	2	3	2	3	2	2	3	2		

Table 25 presents the CSF and cross-walked PF Subcategories for the Incident Recovery Communication (RC.CO) Category. The CSF description for this Category is: Restoration activities are coordinated with internal and external parties.

Table 25. Recover: Incident Recovery Communication (RC.CO).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	1	1	2	1	1	2	1	1	2	2	2	2	Communications help manage trust between all parties processing genomic data. Recovery-related communications inform parties how to appropriately carry out their roles and responsibilities based on the most recent updates for safeguarding data and the genomic data processing environment. Within an organization, executive leadership relies on these communications to stay informed and convey necessary information to partners and stakeholders consistent with leadership responsibilities for managing risk, resources, compliance with laws, and reputation/trust activities, as well as assessing the impact on IP.	1 - Communication throughout the genomic data life cycle helps organizations maintain trust in data quality and improve future outcomes. 2,4,5,9 - Applicable laws and regulations often include communication requirements regarding privacy and consent, such as breach notification. While it may be particularly difficult to contact relatives, organizations will determine what processes need to be developed to communicate with or contact relatives of donors. 7,8 - Recovery communications help organizations, including researchers, repair their reputations and maintain access to trusted data sources.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging.	2	2	2	2	2	2	1	2	2	1	2	2	Managing public relations and providing the public with updates helps maintain trust between partners in the genomic data ecosystem and ensures the future trust of donors, relatives, organizations using genomic data, the public, and the genomic community.	2,7 - Public relations may be the primary way that relatives interact with genomic data. Poor public relations and lack of public updates can impact reputation and whether individuals will trust the organization in the future. Good public relations with timely and clear updates can rebuild and extend trust. 4,5 - Public perception could limit future donors if they do not trust the organization to manage privacy or consent. 8,10,12 - Public perception of researchers, businesses with genomic IP, and new genomic technologies could impact the use and adoption of the organization’s output. Managing public perception promotes trust.

Table 26 presents the Unique PF Subcategories for the Inventory and Mapping (ID.IM-P) Category. The PF description for this Category is: Data processing by systems, products, or services is understood and informs the management of privacy risk.

Table 26. Identify-P: Inventory and Mapping (ID.IM-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	2	2	**1**	2	2	2	2	2	2	3	**1**	2	Knowing whose data is being processed helps determine risks and requirements for provenance, data quality, data access, and legal and regulatory obligations, including compliance with local, state, and national laws.	2 - Additional information on donor data can determine relatives' privacy risks. 3 - Categorizing data contributors from a risk perspective may help identify privacy problems, such as dignity loss, discrimination, loss of trust, or loss of autonomy because of unanticipated revelation of health conditions or progeny. 4 - Actively managing consent for customers' (donors') data ensures compliance with contractual, legal, and ethical requirements or restrictions on data use. 8 - Research data sets, especially for human subjects, can be extensive and high value, requiring appropriate protections. 11 - This is primary information for assessing the appropriate degree of data diversity; the context of processing may require coordination with multiple organizations.
ID.IM-P4: Data actions of the systems/products/ services are inventoried.	**1**	2	**1**	**1**	2	2	2	2	2	2	2	2	Data actions directly impact data provenance and quality and provide context for assessing risks and developing an appropriate authorization schema. Data actions will be clearly communicated	2,5 - Understanding and anticipating harmful data actions mitigates risks or potential harms to donors or relatives. 4 - Data actions that require consent will be known and understood; when data is shared, consent travels with the data and will be applied to define permitted uses of the data.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													across partners and aligned with applicable laws/standards (e.g., GDPR includes purpose limitation and permissible purpose).	11 - Data actions may degrade the diversity of the data, and diversity requirements may impact outcomes.
ID.IM-P5: The purposes for the data actions are inventoried.	2	2	**1**	2	2	2	2	2	2	2	2	2	Data actions' purposes inform identifying potential privacy problems, access controls, legal/regulatory issues, use of technologies, and associated risks that may include identification of relatives, misuse of information, violations of consent, etc.	2,4,5 - This helps protect against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of genomic data. Organizations have a clear purpose for processing data that influences data management, information provided during consent, understanding problematic data actions and harms, etc. Changes in data processing purposes may require updating notices and obtaining updated consent from individuals. 10 - The data processing purpose helps establish and/or trace data ownership and provenance to manage any data actions involving IP. 11 - There is a direct correlation between purpose and determining an appropriate degree of diversity. Inventories of data actions can assist with sample diversity.

Table 27 presents the Unique PF Subcategories for the Business Environment (ID.BE-P) Category. The PF description for this Category is: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.

Table 27. Identify-P: Business Environment (ID.BE-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	2	3	1	2	3	2	2	2	2	2	2	2	This informs the identification of potential risks to data quality, provenance, privacy/consent, access controls, IP protection, data diversity, research data sharing/outcomes, and legal/regulatory compliance. Communicating those requirements promotes effective sharing and trustworthiness.	4 - Manage and communicate consent requirements for genomic systems, products, and services (e.g., failing to obtain consent may result in shutting down a system). 10 - This Subcategory has elevated priority because systems/products/services may be the most likely to contain IP and are key to protecting investments and inventions. 11 - Know which systems/products/services may impact diversity and ensure internal and external collaboration to manage accordingly, even across multiple organizations. 12 - Priorities help define requirements for the technologies used to protect systems/products/services and the genomic data processed.

Table 28 presents the Unique PF Subcategories for the Risk Assessment (ID.RA-P) Category. The PF description for this Category is: The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.

Table 28. Identify-P: Risk Assessment (ID.RA-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).	2	1	1	2	1	2	1	2	2	2	1	1	Genomic data has inherent value. Context is a key factor in assessing data value, helping an organization understand the impact and likelihood of risks to consent, privacy, unauthorized access, research value, and value of IP. Context influences data management strategy and selection of specific privacy-enhancing or security technologies.	3 - Risk assessments will fully integrate contextual factors to protect bioeconomy interests from adverse outcomes to individuals, such as discrimination, exploitation, or abuse, and to organizations, such as reputation or financial. Risks will vary based on technology, quality of data, applicable laws, and partnerships. 7 - Contexts for use include social norms, perceptions, and political issues that factor into managing trust and reputation. Address privacy problems and needs of different subgroups described by context: social, biological, geographic, or other factors that will impact the risk assessment. 11 - Contextual factors include individuals' demographics, a necessary component of evaluating the appropriate degree of diversity. Different populations' genomic data may require additional protections or have different privacy risks that will be factored into risk assessments.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	2	2	2	3	2	3	2	2	3	3	1	3	Bias could impact data quality, research outcomes, and perception of IP. Bias could factor into risks from adverse outcomes to individuals such as discrimination, exploitation, or abuse, and to organizations, such as reputation or financial along with any legal compliance issues.	7 - Bias may impact credibility, positive public perception, and trust. Valid data use and unbiased results will properly reflect the needs of different subgroups described by social, biological, geographic, or other factors, as well as the need to address privacy problems. Not all genomics organizations are creating inputs or using outputs. 8,11 - Bias is critical in the research stage, and in particular for data collected from diverse subject sets. Bias could impact the ability to achieve scientifically valid conclusions and could introduce privacy risks. Evaluating diverse sample sets is needed to avoid unintentional or intentional bias. 12 - Technologies enforce consistent security practices that manage provenance, ensure data quality, restrict access, and understand the impact of bias without introducing any additional bias.

Table 29 presents the Unique PF Subcategories for the Data Processing Ecosystem Risk Management (ID.DE-P) Category. The PF description for this Category is: The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.

Table 29. Identify-P: Data Processing Ecosystem Risk Management (ID.DE-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	2	3	2	3	3	3	3	2	2	3	2	2	These frameworks can help ensure consistency across partners in data quality, provenance, privacy/consent management, access controls, protection of IP, and data diversity, as well as legal/regulatory compliance.	6 - Consider how to control Application Programming Interface (APIs) as well. 7 - Using well-established, robust frameworks can enhance trust. 8 - Researchers sharing data may benefit significantly from improved interoperability to maintain data quality across the ecosystem. 11 - Using standard formats for processing data can help better identify data diversity and any disparities. 12 - Emerging technologies and international standards for data transfer may support interoperability and enhance the use of technologies.

Table 30 presents the Unique PF Subcategories for the Governance Policies, Processes, and Procedures (GV.PO-P) Category. The PF description for this Category is: The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.

Table 30. Govern-P: Governance Policies, Processes, and Procedures (GV.PO-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	2	2	2	1	2	3	2	2	2	3	2	2	Privacy values are operationalized into systems, products, and services by incorporating them into organizational processes that address safeguarding genomic data across the life cycle and ecosystem. Policies directly influence the implementation of data privacy practices and can be used to establish metrics for managing data access and the use of new technologies.	2,5,7 - Determining the privacy risks of 'derived' data from relatives, donors, and trust requires high-level consideration to address potential misperceptions about their value and reach beyond the organization. 4 - Polices are needed to manage consent and re-consent from donors in accordance with permitted uses, sharing with partners, providing notice, protecting secondary data subjects, transparency, and when the right to be forgotten is relevant. 8,10,12 - Researchers and other partners would benefit from clear procedures to manage data quality, provenance, and protections, along with automating security practices wherever possible.

Risk Management Strategy (GV.RM-P) Category: There are no unique PF Subcategories for GV.RM-P; these Subcategories are cross-walked to the following CSF Subcategories: GV.RM-01, GV.RM-02, GV.RM-04, GV.RM-06, and GV.OV-02. The PF description for this Category is: The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Awareness and Training (GV.AT-P) Category: There are no unique PF Subcategories for GV.AT-P; these Subcategories are cross-walked to the following CSF Subcategories: PR.AT-01 and PR.AT-02. The PF description for this Category is: The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.

Table 31 presents the Unique PF Subcategories for the Monitoring and Review (GV.MT-P) Category. The PF description for this Category is: The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.

Table 31. Govern-P: Monitoring and Review (GV.MT-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
GV.MT-P2: Privacy values, policies, and training are reviewed, and any updates are communicated.	3	2	3	3	2	3	3	3	2	3	3	3	Since the risk landscape is constantly changing, the organization will need to keep up by reviewing its values, policies, and training. Otherwise, it risks non-compliance (regulatory) or misalignment with ecosystem partners (contractual) with regards to how it manages its data. These activities may be prioritized when changes introduce a potential impact on privacy that will be communicated across partners.	6 - Managing consent is generally accomplished in the data processing environment. 7 - Privacy policies pertaining to maintaining trust among ecosystem partners are generally accomplished under the Communication function.
GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	2	2	2	2	**1**	3	2	2	**1**	3	3	**1**	Genomic data policies are time-sensitive and location-specific; what is currently adequate to show compliance with regulations may be outdated in a short time or not sufficient in another locale. Organizations that monitor their compliance will be able to demonstrate a high degree of transparency and accountability as trusted partners. Assessing compliance factors in the impact of using new technologies as well as	1,3 - Prioritizing the demonstration of compliance is not a substitute for life cycle risk management. 2,4,5 - Measuring compliance is typically required as part of protecting donors' privacy.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													other changes to the processing environment.	
GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	3	3	2	3	2	3	3	3	3	3	3	3	Implementing the policies will most likely be prioritized above communicating progress. Reporting and communicating progress is standard practice in privacy risk management, and in a genomics community, it is of particular importance to make sure all partners are aligned on risk management; without it, the stakeholders are uninformed.	9 - This may tie into other legal requirements, such as annual reporting or dispute resolution. 8,12 - Communicating progress across partners helps build trust.
GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	**1**	**1**	**1**	3	2	2	2	2	2	3	3	2	Communicating the existence of problematic data actions between partners facilitates response, remediation, and restoration of the data quality and provenance. Each organization needs to address how it manages identification and resolution, whether the source is outside the organization, inside research, or through the research partnership. Communication with impacted donors or relatives helps them determine what actions they can take to protect their own data.	11 - Data diversity may be affected when de-anonymization techniques are discovered and disclosed by a threat actor for a data set of a particular population of interest. 12 - Emerging technologies could introduce problematic data actions. This Subcategory enhances the ability to identify and respond to issues quickly to manage the risks.
GV.MT-P7: Policies, processes, and procedures for receiving, tracking,	2	2	3	2	**1**	3	**1**	2	2	3	**1**	3	Organizations proactively working to receive and respond to feedback from individuals (including donors) will be more responsive to their	2 - An example concern would be when a relative discovers that their information is being used for

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.													needs and concerns, especially in the event that a risk event (as in a data breach) takes place. Responsiveness builds trust in the long term. Failure to be responsive could indicate negligence and destroy trust. Verified issues also result in updates to training and awareness materials.	research and did not consent or has questions about it. 5 - Fair Information Practice Principles (FIPPs) [22] require these processes, including guidance on the secondary data uses that a donor should be aware of. 7 - Potential serious consequences would exist if trust is not handled well.

Table 32 presents the Unique PF Subcategories for the Data Processing Policies, Processes, and Procedures (CT.PO-P) Category. The PF description for this Category is: Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.

Table 32. Control-P: Data Processing Policies, Processes, and Procedures (CT.PO-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	**1**	2	**1**	**1**	**1**	**1**	2	2	**1**	2	3	**1**	Authorization assigns accountability and responsibility for data processing. This process ensures that the operating environment incorporates privacy-related requirements for data quality, provenance, risk management, consent, data access, and data sharing.	2,5 - Authorization operationalizes governance and risk management decisions, considering risk to relatives and donors throughout data processing. 3,6 - Data processing policies are one of the key outcomes for this mission objective. 4 - Authorization processes ensure that accountability for policies and processes for managing consent is in place and included in data-sharing agreements. 7 - Proper authorization processes build trust by ensuring that accountability for data processing is in place. 9 - "Authorization to Operate" processes help assign and enforce legal and regulatory responsibilities for the organization.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality and manage data retention).	**1**	**1**	2	**1**	**1**	**1**	2	2	2	2	2	**1**	Effective data management, data sharing, and data processing policies and procedures help implement risk management measures and alignment with donor expectations. They protect against data loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of genomic data, which helps organizations comply with laws and regulations while building trust and confidence between organizations sharing data.	2 - Relatives do not have an opportunity to provide consent and will be able to request that their data is not shared and is properly deleted. 4 - This is necessary to ensure that data is processed in a manner consistent with consent. 6 - Ensure that both internal and external stakeholders understand data access requirements. 11 - This may make it more likely that a diverse group of donors will participate. 12 - This sets the stage for technical privacy capabilities like PETs.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	2	2	2	2	**1**	2	2	2	2	3	2	2	Enabling individual data preferences supports the implementation of common privacy requirements by establishing controls to match policies. Policies, processes, and procedures will align and enforce donor preferences and consent. Consistency will promote trust and encourage diverse donor participation.	2,4,5 - Donors and relatives will be able to request data deletion. If included in consent, donors may have individual preferences for participation in data sharing. 7 - Honoring individual preference supports and reflects the needs of different subgroups described by social, biological, geographic, or other factors, and addresses privacy problems. 6 - This aligns access controls with an individual's preferences and will dictate access rights. 8 - This promotes privacy objectives but can run counter to research objectives.

Table 33 presents the Unique PF Subcategories for the Data Processing Management (CT.DM-P) Category. The PF description for this Category is: Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).

Table 33. Control-P: Data Processing Management (CT.DM-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.DM-P1: Data elements can be accessed for review.	**1**	3	3	2	2	3	2	2	2	3	3	2	Data element access will be managed appropriately to ensure data quality and provenance and to conform to consent requirements. Unauthorized data element access may jeopardize trust and can be managed by using PETs. Privacy requirements include an individual's ability to review information held about them.	2,5 - Limiting data element access supports data minimization and can help prevent the risk of identifying relatives. 4 - Access follows donor consent requirements. 7 - Original data can be reviewed to identify bias in results. 8 - Since genomic data is typically in human-readable format, data element access will be managed while it is made available for research.
CT.DM-P2: Data elements can be accessed for transmission or disclosure.	2	3	3	2	2	3	3	2	2	3	3	2	This is a similar priority to CT.DM-P1, with additional considerations for data sharing. Priority for this Subcategory would be protecting sensitive data and managing disclosure (IP, consent, etc.) for authorized purposes.	4 - Consent requirements travel with genomic data. Access to data elements is required for sharing clinical data across systems. 9 - This supports compliance where sharing is required. 12 - PETs support confidential data sharing and transmission.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.DM-P3: Data elements can be accessed for alteration.	**1**	3	3	3	2	3	3	3	2	3	3	2	Data alteration can directly impact data quality, provenance, consent, IP, and research outcomes and reliability. Therefore, alterations will be closely managed and monitored. Alterations may be required to update privacy-related information and address errors, and for research purposes.	4 - The donor needs to be able to correct, update, and amend data, and make changes to consent when applicable. 5 - Donor information will be altered or amended if the data changes (e.g., data changes due to viruses or treatments). 9 - GDPR and other regulations require the ability to amend data. Organizations need to respond to requests for amendment or correction.
CT.DM-P4: Data elements can be accessed for deletion.	**1**	2	2	2	2	3	2	3	2	2	3	2	Data deletion supports privacy measures like the removal of old data when it is no longer needed, the right to be forgotten, and proper deletion consistent with consent. Some of these measures are legally required (e.g., GDPR).	2 - Since relatives don't have an opportunity to provide consent, they should be able to request that their data be deleted. 4 - Data will be managed in a way that is consistent with what the donor consented to. Access and the reason for access will be consistent with the consent given. 5 - Organizations put in place mechanisms to allow donors to delete their information (especially in cases of a breach). If a donor's consent changes, data will be destroyed in a way that is consistent with policies in place to protect privacy. 7 - A violation of trust occurs if information is not deleted as required.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														9 - Deletion is required to comply with applicable laws and regulations, including retention schedules, when requested by the individual (e.g., GDPR's right to be forgotten).
CT.DM-P6: Data are transmitted using standardized formats.	**1**	3	2	2	2	2	2	2	3	3	3	2	Standardized formats enable easier management of data quality and provenance while helping reduce risk by limiting confusion and the amount of data processing necessary to get data into a usable format.	4 - Standardization helps manage consent since consent requirements travel with genomic data. 8 - Standardized formats enhance and improve data sharing in research communities, while non-standardized formats could negatively impact the reproducibility of a study. 11 - Using standard formats for processing data can help better identify disparities. 12 - Standard formats help reduce risk and errors, which can be an important factor with MPC and other PETs in research and data sharing.
CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.	**1**	2	2	2	2	**1**	3	2	**1**	2	2	2	Processing permissions facilitates management of data provenance, quality, and access while managing risk to individuals and the organization by ensuring that requirements (e.g., consent) travel with the data. Data element access and transmission are basic elements for sharing clinical	2,4,5,7 - Privacy requirements, including consent and permissions to conduct research, travel with the data and support data minimization and trust that permissions are enforced. 6 - Properly managing permissions and consent without impacting necessary activities such as data analysis is an important aspect of data access.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
													data across systems and the broader research community.	10 - Permissions help establish and/or trace data ownership and provenance for IP.
CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.	2	3	3	3	2	3	3	3	3	3	3	2	Testing data management measures helps determine if there are issues that may impact data quality, provenance, privacy, access, and IP protections. Testing can be used to verify that consent and other privacy requirements are met.	9 - Data processing management and testing is informed by the Fair Information Practice Principles to comply with most regulations. 12 - Additional testing and assessment steps are needed to ensure that new technologies meet specifications. Over-processing and repeated analyses can lead to errors and re-identification.
CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives, and outputs are evaluated against these preferences.	3	2	3	2	**1**	2	2	2	2	3	2	2	Protecting privacy preferences in algorithmic design can help enforce privacy protections and manage data access in compliance with consent. Privacy engineering practices can leverage the privacy preferences in the algorithms to support privacy requirements.	2,4,5,11 - Given the increase in algorithmic decision-making, this Subcategory is a priority for managing donors' privacy, relatives' privacy, consent, trustworthiness, and data diversity. 6 - Preferences correspond to access controls, defining ways to fine-tune access controls in higher risk scenarios. 7 - Algorithms can be tailored to reflect the needs of different subgroups described by social, biological, geographic, or other factors, and to address specific privacy problems.

Table 34 presents the Unique PF Subcategories for the Disassociated Processing (CT.DP-P) Category. The PF description for this Category is: Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).

Table 34. Control-P: Disassociated Processing (CT.DP-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CT.DP-P1: Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).	2	2	2	2	2	2	3	2	**1**	3	2	2	Organizations can preserve original source and privacy rights over time using disassociated processing that limits observability and linkability to reduce data exposure (impacting privacy and consent) and associated risks.	2,4,5 - Disassociated processing facilitates data minimization and reduces exposure of donors and relatives in accordance with consent. 6 - Facilitating granular data access helps prevent unauthorized access. 9,12 - As new technologies emerge with promises of limiting data exposure and linkages, verification of their effectiveness and compliance with legal requirements will need to be demonstrated. 10 - This capability could support the protection of IP while it is being used.
CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).	2	**1**	2	2	**1**	3	2	2	**1**	3	2	2	These technologies restrict donor identification to only those with a legitimate need to know, promoting data minimization, reducing the risks of unwanted identifiability, and preserving the provenance of the original data source and privacy rights over time.	2,4,5 - This decreases the risk of donor/relative identification while providing data access as specified by the individual who gave consent for the use of their data. 8 - Disassociated processing can help reduce risk when sharing data, making it easier for researchers to follow principles like data minimization.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														9 - This is an important component of privacy by design, which can build in legal and regulatory compliance. 11 - This is important for under-represented or vulnerable populations, or those who may be targeted.
CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	3	2	3	2	2	3	2	2	**1**	3	3	2	This Subcategory minimizes the impact that can result from having access to data about individuals and the potential for individuals to become targeted or experience privacy harms. As new technologies and techniques become available, even existing data may be used in ways not previously envisioned or described through consent.	2,4,5 - Protect donors and relatives by minimizing the impact that can result from having access to this data and individuals potentially becoming targeted or experiencing privacy harms. Consent agreements may need to be expanded when these inferences are being drawn. 7 - Be cautious with inferences, even when accurate, that may reveal bias or loose data exposure practices. 9 - Prioritize to comply with various laws and regulations like GDPR, CPRA [23], and others. 12 - Emerging technologies may support conclusions about individuals that were previously unavailable.
CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	2	2	2	2	2	**1**	3	2	2	3	3	2	Device configurations can enforce data exposure to only what is necessary, enforcing data access and data provenance requirements and reducing associated risks throughout the data life cycle.	4 - Configuration can help enforce consent, which travels with the data, and enable privacy protections by letting some users see only part of the data. 6 - These configurations enforce data minimization and granular management of data access controls.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
														9 - Specific configurations support the common privacy principle of minimization in compliance with laws and regulations.
CT.DP-P5: Attribute references are substituted for attribute values.	3	2	3	3	2	3	3	3	2	3	3	2	Substituting attribute references is a best practice to limit exposure to privacy risks to protect individuals, preserve consent, and minimize data exposure. It is a context-specific decision for when and how to do it.	2,4,5 - This minimizes the ability to recombine data to re-identify a donor or relative. 9 - Pseudonymization of data is part of privacy by design and supports laws and regulations. 12 - When implementing emerging technologies, practices like this can be used to enhance privacy but will be thoroughly tested to ensure they are not reversible.

Table 35 presents the Unique PF Subcategories for the Communication Policies, Processes, and Procedures (CM.PO-P) Category. The PF description for this Category is: Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.

Table 35. Communicate-P: Communication Policies, Processes, and Procedures (CM.PO-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	2	3	2	2	2	2	2	2	3	3	2	2	This Subcategory was not as high a priority as performing the communication (CM.PO-P1). Communication roles and responsibilities help organizations clearly communicate what communication is expected by who, when, and with what result. Communication requirements will dictate what needs to be done when, but these requirements will then be carried out by personnel who understand the value of communication in managing trust.	7 - The workforce and partner organizations will understand how and under what circumstances to communicate to donors, partners, and the public. 8 - The value of research results relies on data integrity and trust between partners.

Table 36 presents the Unique PF Subcategories for the Data Processing Awareness (CM.AW-P) Category. The PF description for this Category is: Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.

Table 36. Communicate-P: Data Processing Awareness (CM.AW-P).

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	2	2	2	**1**	**1**	2	**1**	2	2	3	2	2	Mechanisms will be in place to reach donors and, when possible, affected relatives. Organizations need clear communication protocols to manage consent changes and maintain their reputation. Coordination among organizations fosters trust and ensures consistent security practices.	4,5 - Organizations provide clear and accurate information to donors on the consent process, including any changes to how their data is being used, how donors can withdraw consent, and the process for requesting changes to how their consent may be used.
CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.	2	3	2	2	2	2	2	2	3	3	2	3	Feedback mechanisms help organizations identify any issues with data use. This Subcategory can be prioritized by organizations when they are trying to build or rebuild the trust of donors or other users of their data.	5 - These mechanisms can create a feedback look when privacy events or incidents occur to engage donors. 7 - Surveys can be tailored to reflect the needs of different subgroups described by social, biological, geographic, or other factors. Providing individuals with a true voice in the process can foster trust.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CM.AW-P3: System/product/service design enables data processing visibility.	**1**	2	2	2	2	2	3	3	2	3	3	2	Visibility into data processing ensures compliance with applicable laws and consent agreements and will support reputational trust as well as provide a way to verify data quality and provenance. Data processing will be managed according to consent.	6 - Visibility requirements define who needs to access the data, which informs how access controls are implemented. Monitoring provides details on who actually accessed the data to enforce accountability.
CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/ disclosure.	**1**	2	2	2	**1**	2	2	2	**1**	2	2	2	Data disclosure records can be used to verify access and determine any potential issues with data quality, provenance, or unauthorized access that may result in data leaks. Organizations will report who accessed sensitive data to comply with laws, contracts, data-sharing agreements, and consent requirements.	3,5 - Records enable audits and provide accountability for access that may result in adverse outcomes to individuals, such as discrimination, exploitation, or abuse, and to organizations, such as reputation or financial. 4,7,8,9 - Records provide accountability and traceability to build trust by confirming that data processing is occurring as designed and that consent is properly managed and remains in sync over time, such as when technologies enable new processing capabilities or when genomic data is shared with new partners. This relates to the "privacy by design" priority in GDPR. 12 - Controlling data downloading supports technology assessments and PETs, contributing to accountability and record-keeping.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	**1**	2	2	2	2	2	2	2	2	3	2	2	Individuals will be allowed to make corrections and deletions to their privacy-related information to manage data quality and enforce privacy requirements from consent to the right to be forgotten. Donors can withdraw participation and want to know that their data is handled consistently with the consent they provided. This Subcategory helps organizations manage reputational risk and compliance with regulations.	2 - Deletion is one way that relatives can manage their data since they can't give consent or even verify if their information is correct. 4 - Corrections and deletions of data will be permitted in accordance with individual preferences and the relevant retention schedule.
CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/ disclosure.	**1**	2	2	2	2	2	2	2	2	2	2	2	Ensuring the integrity of the chain of provenance enforces accountability, protects data quality throughout processing, and provides an assurance to donors that their information is processed according to consent. Records can be used for accountability on who accessed the data and for determining any risks to data quality or provenance.	12 - This may be included as a requirement for new technologies.

Subcategory	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Tech	General Rationale	Mission Objective Specific Considerations
CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	2	**1**	2	**1**	**1**	3	**1**	2	**1**	3	2	3	Organizations are legally required to notify individuals and organizations affected by a breach. Breach response processes will be regularly reviewed and updated to manage risks effectively and maintain compliance and trust. Donors, particularly from under-represented groups, may withdraw their information or be hesitant to share their data when they can't trust an organization to communicate appropriately.	2,4,5 - It may be impossible to notify relatives, but response plans will assess who needs to be notified, how they will be notified, and how soon. Then, donors will need to be able to update their consent, verify the accuracy of their data, and take any other actions needed to manage their personal data and privacy risks. 7 - This is one way that organizations can manage their reputational risk to maintain credibility and a positive public perception. 9 - Organizations will know and comply with any laws and regulations that require breach notification.
CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address the impacts of problematic data actions.	2	2	2	2	2	3	**1**	2	2	3	2	3	Along with notification, donors will be able to mitigate the risks associated with a breach. These mitigation mechanisms may promote trust and reputation.	7 - This is one way that organizations can manage their reputational risk to maintain credibility and a positive public perception. However, the value of specific mechanisms may change over time and will be reviewed. 9 - Organizations will know and comply with any laws and regulations that require these mitigation mechanisms.

Protect-P Categories: There are no unique PF Subcategories for the Protect-P Function; these Subcategories are cross-walked to CSF Subcategories in other tables. Please refer to the Genomic Data Profile Spreadsheet Tool for details of all Subcategories that do not appear in this crosswalk from CSF to PF.

References

[1] National Institute of Standards and Technology (2024) The Cybersecurity Framework (CSF) 2.0 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 29. https://doi.org/10.6028/NIST.CSWP.29

[2] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[3] National Cybersecurity Center of Excellence (2022) NCCoE Virtual Workshop on the Cybersecurity of Genomic Data. Available at https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-virtual-workshop-cybersecurity-genomic-data

[4] National Cybersecurity Center of Excellence (2022) NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data. Available at https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-virtual-workshop-exploring-solutions-cybersecurity-genomic-data

[5] Pulivarti R, Martin N, Byers F, Wagner J, Maragh S, Wilson K, Wojtyniak M, Kreider B, Frances A, Edwards S, Morris T, Sheldon J, Ross S, Whitlow P (2023) Cybersecurity of Genomic Data. (National Institute of Standards and Technology, Gaithersburg, MD), Initial Public Draft NIST Interagency or Internal Report (IR) 8432. https://doi.org/10.6028/NIST.IR.8432.ipd

[6] Executive Order 14081 (2022) Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy. (The White House, Washington, DC), 87 FR 56849, September 12, 2022. https://www.govinfo.gov/app/details/FR-2022-09-15/2022-20167

[7] Naveed M, Ayday E, Clayton EW, Fellay J, Gunter CA, Hubaux J-P, Malin BA, Wang X (2015) Privacy in the Genomic Era. *ACM Computer Survey* 48(1):1-49. https://doi.org/10.1145/2767007

[8] US Office of Science and Technology Policy (2023) Visions, Needs, and Proposed Actions for Data for the Bioeconomy Initiative Final Report (The White House, Washington, DC), December 2023. Available at https://www.whitehouse.gov/wp-content/uploads/2023/12/FINAL-Data-for-the-Bioeconomy-Initiative-Report.pdf

[9] Erlich Y and Narayanan A (2014) Routes for breaching and protecting genetic privacy. *Nature Reviews Genetics* 15:409-421. https://doi.org/10.1038/nrg3723

[10] Erhlich Y, Shor T, Pe’er I, Carmi S (2018) Identity Inference of Genomic Data Using Long-Range Familial Searches," *Science* 362(6415):690-694. https://doi.org/10.1126/science.aau4832

[11] Schwab A, Juu HS, Wang J, Park JY (2018) Genomic Privacy. *Clinical Chemistry* 64(12):1696-1703. https://doi.org/10.1373/clinchem.2018.289512

[12] Gianfrancesco M, Tamang S, Yazdany J, Schmajuk G (2019) Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data. *JAMA Internal Medicine* 178(11):1544-1547. https://doi.org/10.1001/jamainternmed.2018.3763

[13] Joly Y, Dalpé G, Dupras C, Bévière-Boyer B, de Paor A, Dove ES, Moreno PG, Ho CWL, Ho C-H, Ó Cathaoir K, Kato K, Kim H, Song 3, Minssen T, Nicolás P, Otlowski M, Prince AER, Nair APS, Van Hoyweghen I, Voigt TH, Yamasaki C, Bombard Y (2020) Establishing the International Genetic Discrimination Observatory. *Nature Genetics* 52:466-468. https://doi.org/10.1038/s41588-020-0606-5

[14] Parikh RB, Teeple S, Navathe AS (2019) Addressing Bias in Artificial Intelligence in Health Care. *JAMA* 1 322(24):2377-2378. http://doi.org/10.1001/jama.2019.18058

[15] The National Counterintelligence and Security Center (2021) China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security. (The National Counterintelligence and Security Center, Washington, DC), pp 1-5. Available at NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf (dni.gov) dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf

[16] Health Insurance Portability and Accountability Act of 1996, Pub. 3. 104-191, 110 STAT. 1936. https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[17] Federal Information Security Modernization Act of 2014, Pub. 3. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283/

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 3 119, 4.5.2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504

[19] Genetic Information Nondiscrimination Act of 2008, Pub. 3. 110-233, 122 Stat. 811. https://www.govinfo.gov/app/details/PLAW-110publ233

[20] 21st Century Cures Act of 2016, Pub. 3. 114-255, 130 Stat. 1033. https://www.govinfo.gov/app/details/PLAW-114publ255#:~:text=Document%20Citations&text=21st%20Century%20Cures%20Act%2C%20Pub,%2Fdetails%2FPLAW%2D114publ255

[21] Cybersecurity & Infrastructure Security Agency (2021) Binding Operational Directive 22-01. Available at https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01

[22] OECD (2002), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (OECD Publishing, Paris). https://doi.org/10.1787/9789264196391-en

[23] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=**1**.81.5

[24] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[25] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[26] Barker EB, Roginsky AL, Davis R (2020) Recommendation for Cryptographic Key Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-133, Rev. 2. https://doi.org/10.6028/NIST.SP.800-133r2

[27] NIH National Human Genome Research Institute (2023). NHGRI Talking Glossary of Genomic and Genetic Terms. Available at https://www.genome.gov/genetics-glossary

[28] Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau D (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

[29] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

[30] Oldehoeft AE (1992) Foundations of a Security Policy for Use of the National Research and Educational Network. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 4734. https://doi.org/10.6028/NIST.IR.4734

[31] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

Appendix A. Selected Bibliography

- Cybersecurity and Privacy Reference Tool (CPRT) https://csrc.nist.gov/Projects/cprt
- CSF Informative References https://www.nist.gov/informative-references
- National Online Informative References (OLIR) Program https://csrc.nist.gov/projects/olir
- Privacy Framework Resource Repository https://www.nist.gov/privacy-framework/resource-repository

Appendix B. List of Symbols, Abbreviations, and Acronyms

The following acronyms are used in this publication.

AC
Access Control

AE
Anomalies and Events

AM
Asset Management

AN
Analysis

API
Application Programming Interface

AT
Awareness and Training

BE
Business Environment

BIO-ISAC
Bioeconomy Information Sharing and Analysis Center

CM
Security Continuous Monitoring

CPRA
The California Privacy Rights Act (2020)

CO
Communications

CSF
NIST Cybersecurity Framework

CTI
Cyber Threat Intelligence

DbGaP
Database of Genotypes and Phenotypes

DE
Detect

DNA
Deoxyribonucleic acid

DP
Detection Processes

DS
Data Security

EO
Executive Order

FISMA
Federal Information Security Modernization Act (2014)

GDRP
General Data Protection Regulation (2016)

GINA
Genetic Information Nondiscrimination Act (2008)

GDPR
General Data Protection Regulation

GxP
Good Practices

GV
Governance

HIPAA
Health Insurance Portability and Accountability Act (1996)

ID
Identify

IM
Improvements

IP
Information Protection Processes and Procedures

IP
Intellectual Property

ISACs
Information Sharing Analysis Centers

ITL
Information Technology Laboratory

MA
Maintenance

MI
Mitigation

MO
Mission Objective (only used in the Tables)

NCBC
National Centers for Biomedical Computing

NCBI
National Center for Biotechnology Information

NCCoE

NIST National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

NIST IR
NIST Internal Report

PETs
Privacy-Enhancing Technologies

PF
Privacy Framework

PII
Personally Identifiable Information

PHI
Protected Health Information

PR
Protect

PT
Protective Technology

RA
Risk Assessment

RC
Recover

RM
Risk Management Strategy

RP
Recovery Planning

RP
Response Planning

RS
Respond

SBOM
Software Bill of Materials

SC
Supply Chain Risk Management

SRA
Sequence Read Archive

TTPs
Tactics, Techniques, and Protocols

Appendix C. Glossary

Asset
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes [24].

Cybersecurity Event
A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation) [25].

Data Integrity
A property possessed by data items that have not been altered in an unauthorized manner since they were created, transmitted, or stored [26].

Genome
The entire set of DNA instructions found in a cell. In humans, the genome consists of 23 pairs of chromosomes located in the cell's nucleus, as well as a small chromosome in the cell's mitochondria. A genome contains all the information needed for an individual to develop and function [27].

Network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices [28].

Problematic Data Action
A data action that could cause an adverse effect for individuals [2].

Provenance
The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data [29].

Sensitive Data
A descriptor of information whose loss, misuse, or unauthorized access or modification could adversely affect security [30].

System
A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [31].