OT BACKUP QUICK START GUIDE

Operational Technology (OT) backups are a vital component of any organization's response and recovery effort, critical in maintaining reliable system operation, continuing critical functions, and recovering from cyber incidents (*RC.RP-03, 04, RC.CO-03). Effective backup management in an OT environment involves integrating backups into the change and risk management processes, creating them regularly, testing them, and reviewing them during recovery exercises (PR.DS-11, RC.RP-02). Organizations should also consider infrastructure dependencies when developing an OT backup strategy.

PREREQUISITES

- Identify all OT devices that contain important configurations or support process operation (e.g., Programmable Logic Controllers (PLCs), switches, firewalls, transmitters, actuators, Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) servers, Variable Frequency Drives (VFDs), Human Machine Interfaces (HMIs)) (ID.AM-01).
- Verify the asset inventory is current and assign mission criticality to prioritize your backup frequency, retention policies, and recovery sequence (ID.AM-05).

IDENTIFY ASSETS CRITICAL TO OPERATIONS

- Identify the files, software applications, and spare parts required to restore the environment (e.g., program files, logic files, configuration files and details, Input/Output (I/O) lists, firmware, graphics (HMI) files, license keys, vendor configuration tools, support documentation, operating system or virtual machine images, supporting software required for redeployment) (ID.AM).
- Create a spare parts plan that ensures the availability of critical components to meet the recovery time objectives, mitigates supply chain delays, and includes hardware that is compatible with the digital backups (GV.SC-02, 04, 05, 07, 09, PR.IR-03).

IDENTIFY BACKUPS REQUIRED FOR EACH ASSET

- Define frequency, media, and storage location(s) based on how often information changes, system type, and risk (GV.PO-01).
- Document OT-specific backup constraints and risks (particularly those associated with legacy equipment, such as availability and a lack of security features) and account for them in your backup and recovery approach (ID.RA-01, 04, 05, 06).
- Use the organization's change management process to review and approve backup-impacting changes (GV.PO-02, ID.RA-07, PR.PS-01).
- Establish media labeling and indexing procedures that include details such as system name, date, and time (ID.AM).
- Define requirements for maintaining redundant backup storage both on-site and off-site (PR.IR-03).
- Determine mechanisms to maintain the integrity and availability of backups (e.g., hashing, encryption, write-once media) (PR.IR-03). When using encryption, follow industry best practices regarding encryption algorithms and key management. See NIST SP 1334 for more information.
- Establish the methods for protecting backup media from unauthorized access, modification, and destruction (PR.DS).

NIST Special Publication
SP 1339
https://doi.org/10.6028/NIST.SP.1339
June 2026

Additional guidelines found in:
NIST SP 800-82 Rev. 3 (https://doi.org/10.6028/NIST.SP.800-82r3)
NIST SP 1800-11 (https://doi.org/10.6028/NIST.SP.1800-11)
*NIST Cybersecurity Framework (CSF) 2.0 (https://doi.org/10.6028/NIST.CSWP.29)

MANAGE PROCEDURES FOR BACKUP AND RECOVERY

- Acquire vendor manuals, software utilities, and technical guidance to support backup and recovery operations. Adapt and integrate these recommended procedures into the organization's backup, recovery, and change management processes to ensure alignment with specific operating environments and safety requirements (GV.PO-01, 02).
- Maintain specialized engineering software, cables, and licenses required for immediate response onsite (PR.IR-03, RC.RP-05).
- Create a procedure for storing file hashes of backup content to use for verification before restoration processes are executed (PR.DS, PR.IR-03, RC.RP-03).
- Use hot backups for immediate failover with real-time replication. Implement warm backups for quick recovery with regularly updated data. Utilize cold backups for offline data (e.g., logical) or spare parts (e.g., physical) that require a full rebuild before service is restored (RS.AN-08, RC.RP-05).

BACKUP INTEGRITY TESTING AND RESTORATION

- Conduct recurring restoring tests of backups on non-production systems to validate backup media reliability, practice restoration procedures, and verify the functional integrity of the restored system (PR.DS-11).
- Ensure backup integrity via cryptographic hashing where feasible. For OT assets, validate integrity using approved engineering methodologies like offline-to-online logic comparisons or native software verification (RC.RP-03).
- Update backup and restoration processes, procedures, and documentation based on lessons learned during the testing process to improve recovery speed during an actual emergency (RC.RP-06, RC.CO).

SAVE ENGINEERING DOCUMENTS FOR A LAYERED APPROACH TO RECOVERY PREPARATION

- On a recurring basis, ensure supplemental documents are available in both printed and electronic formats to support incident response requirements (PR.IR-03).
- Maintain documents that can help expedite verification, validation, and troubleshooting during system restoration (e.g., logic print files, I/O lists, equipment specification sheets, Safety Requirements Specifications (SRS), control narratives, Cause and Effect Matrices, network diagrams, wiring diagrams, historian configurations).

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about NCCoE Manufacturing, visit: https://www.nccoe.nist.gov/manufacturing

@NISTcyber

linkedin/showcase/nccoe

NIST Special Publication
SP 1339
https://doi.org/10.6028/NIST.SP.1339
June 2026

Additional guidelines found in:
NIST SP 800-82 Rev. 3 (https://doi.org/10.6028/NIST.SP.800-82r3)
NIST SP 1800-11 (https://doi.org/10.6028/NIST.SP.1800-11)
*NIST Cybersecurity Framework (CSF) 2.0 (https://doi.org/10.6028/NIST.CSWP.29)