CRITICAL INFRASTRUCTURE

STIG

# Operational Resilience Checklist

A forward-facing, high-level checklist designed to reduce downtime risk, strengthen incident readiness, and modernize security operations across IT and OT environments.

Version: 1.0 | Date: February 13, 2026

Use this checklist as a readiness guide. It is not legal advice and should be tailored to your organization's environment, sector requirements, and risk profile.

## Cyber Resilience for Organizations That Can't Go Down

In critical infrastructure, a cyber incident is rarely "just a data event." It can disrupt services, create safety impacts, and trigger public trust and regulatory consequences. This checklist helps organizations focus on the controls and practices that most directly protect uptime and recovery.

The checklist is aligned to commonly used resilience and cybersecurity frameworks and emphasizes measurable, operational outcomes over "check-the-box" compliance.

### Top Resilience Risks We See in Critical Infrastructure

- Downtime and crisis gaps: No practiced playbook for when operations are disrupted or degraded.
- Tool sprawl: Disjointed IT and OT environments with overlapping or unmanaged security tools.
- Visibility blind spots: Unmanaged endpoints, weak segmentation, incomplete asset inventories, and limited OT telemetry.
- Third-party exposure: Vendor remote access and support pathways that are not tightly governed or monitored.

### Forward-Looking Drivers

Resilience expectations are rising across critical infrastructure. Many organizations are aligning to CISA's Cross-Sector Cybersecurity Performance Goals (CPG 2.0) as a baseline, and to NIST CSF 2.0 for governance, risk management, and recovery outcomes.

# CRITICAL INFRASTRUCTURE

Forward-facing programs are also adopting “cyber-resilient by design” principles: segmentation, redundancy, secure remote access, immutable recovery paths, and repeatable exercises that reduce Mean Time to Recovery (MTTR).

## Future-Ready Focus Areas

- Measurable baseline controls aligned to CPGs and sector requirements (IT and OT).
- Asset and access rigor: inventories, identity controls, privileged access management, and vendor remote access governance.
- Resilient architecture: segmentation, fail-safe designs, and tested recovery for critical services.
- Operationalized incident response: clear decision-making, communications, containment, and recovery playbooks.
- Third-party and supply chain resilience: enforceable requirements, monitoring, and contingency plans.

## How to Use This Checklist

- Assess: Mark each item as In Place, Partial, or Not In Place.
- Plan: Convert gaps into a prioritized roadmap (people, process, technology) tied to operational impact.
- Build: Implement controls in a way that respects OT safety and uptime constraints.
- Validate: Test with tabletop exercises, technical recovery drills, and penetration testing/validation.
- Maintain: Re-validate at least annually and after major changes, incidents, or significant new threats.

## Scope and Inputs

Before starting, confirm scope: the services that must remain available, the OT/IT systems that enable those services, external dependencies (telecom, cloud, SaaS, vendors), and the safety/regulatory impacts of disruption.

# CRITICAL INFRASTRUCTURE

STIG

## 1. Governance and Accountability

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Executive sponsor and resilience charter are established | Charter defines objectives (uptime, safety, compliance), scope, and decision rights. | In Place / Partial / Not In Place |
| ☐ Critical service owners are assigned with documented RACI | Service ownership spans IT, OT, facilities, comms, and vendors as applicable. | In Place / Partial / Not In Place |
| ☐ Risk appetite for downtime and safety impact is documented | Defines acceptable outage windows, safety constraints, and escalation thresholds. | In Place / Partial / Not In Place |
| ☐ Program maps to baseline frameworks (CPG 2.0, CSF 2.0) | Control mapping supports consistent reporting and investment prioritization. | In Place / Partial / Not In Place |
| ☐ Resilience metrics are defined and reviewed regularly | Track MTTD/MTTR, patch coverage, MFA adoption, backup health, and incident trends. | In Place / Partial / Not In Place |
| ☐ Evidence repository exists for audits and insurer requests | Central store for policies, procedures, test results, and control evidence. | In Place / Partial / Not In Place |
| ☐ Exception process exists with approvals and expirations | Risk-accepted exceptions have owners, compensating controls, and expiry dates. | In Place / Partial / Not In Place |
| ☐ Budget and roadmap align to operational impact | Roadmap prioritizes improvements that reduce downtime likelihood and duration. | In Place / Partial / Not In Place |

## 2. Critical Services, Dependencies, and Impact

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Business Impact Analysis (BIA) covers operational and safety impacts | BIA includes financial, regulatory, safety, and public trust consequences. | In Place / Partial / Not In Place |
| ☐ Recovery objectives are defined per critical service (RTO/RPO) | Targets reflect realistic restoration capability and business needs. | In Place / Partial / Not In Place |
| ☐ Dependency mapping is maintained for critical services | Maps OT/IT systems, identities, networks, vendors, and facilities dependencies. | In Place / Partial / Not In Place |
| ☐ Single points of failure are identified and addressed | Redundancy plans exist for critical components and communications paths. | In Place / Partial / Not In Place |
| ☐ Manual or degraded-mode procedures are documented and trained | Fallback workflows keep services running safely during partial outages. | In Place / Partial / Not In Place |
| ☐ Data flows and trust boundaries are documented | Shows where control signals, telemetry, and sensitive data traverse networks. | In Place / Partial / Not In Place |
| ☐ Crisis communications plan includes internal and external | Includes regulators, customers, partners, and public messaging processes. | In Place / Partial / Not In Place |

| | | |
|---|---|---|
| stakeholders | | |
| ☐ Exercises include leadership decision-making and cross-team coordination | Tabletops test escalation, comms, and operational continuity decisions. | In Place / Partial / Not In Place |

## 3. Asset, Identity, and Access Foundations

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ IT and OT asset inventories are complete and maintained | Inventory includes owner, location, criticality, OS/firmware, and connectivity. | In Place / Partial / Not In Place |
| ☐ Asset criticality and segmentation zones are defined | Critical assets are tagged and placed into appropriate security zones. | In Place / Partial / Not In Place |
| ☐ Secure configuration baselines are implemented and monitored | Hardened builds exist for servers, endpoints, network devices, and OT hosts. | In Place / Partial / Not In Place |
| ☐ Unique user accounts and least-privilege access are enforced | Shared accounts eliminated or strictly controlled; periodic access reviews. | In Place / Partial / Not In Place |
| ☐ Privileged Access Management (PAM) is used for admin access | Admin sessions are controlled, logged, and time-bound where feasible. | In Place / Partial / Not In Place |
| ☐ Multi-factor authentication protects remote and administrative access | MFA covers VPN/ZTNA, admin consoles, cloud portals, and privileged tools. | In Place / Partial / Not In Place |
| ☐ Vendor remote access is tightly governed and monitored | Just-in-time approvals, segmentation, session logging, and rapid offboarding. | In Place / Partial / Not In Place |
| ☐ IT/OT segmentation and a managed OT DMZ are implemented | Segmentation reduces blast radius and limits lateral movement pathways. | In Place / Partial / Not In Place |
| ☐ Wireless and rogue access point risks are managed | Wireless controls include approved configurations and monitoring for rogue APs. | In Place / Partial / Not In Place |
| ☐ Physical access controls support cyber resilience | Critical spaces have access control, visitor logging, and environmental safeguards. | In Place / Partial / Not In Place |

## 4. Monitoring, Detection, and Response Operations

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Centralized logging exists for critical IT and OT-adjacent systems | Logs are retained, searchable, and protected from tampering. | In Place / Partial / Not In Place |
| ☐ Time synchronization is consistent across critical systems | NTP sources are defined; log timestamps are reliable for investigations. | In Place / Partial / Not In Place |
| ☐ Detection use cases prioritize | Ransomware, remote access abuse, privilege | In Place / Partial / |

| | | |
|---|---|---|
| high-impact threats | escalation, and OT disruption scenarios. | Not In Place |
| ☐ Monitoring coverage and response expectations are defined | 24/7 or defined response windows with clear escalation and on-call procedures. | In Place / Partial / Not In Place |
| ☐ Response playbooks exist for high-impact scenarios | Containment and recovery steps are documented for IT and OT contexts. | In Place / Partial / Not In Place |
| ☐ Endpoint detection and containment is available for critical endpoints | EDR supports isolation/quarantine, triage, and forensic collection. | In Place / Partial / Not In Place |
| ☐ Network visibility supports east-west monitoring and segmentation validation | Network telemetry enables detection of lateral movement and policy violations. | In Place / Partial / Not In Place |
| ☐ Incident severity includes operational impact and safety considerations | Severity model accounts for downtime risk, safety, and public impact. | In Place / Partial / Not In Place |
| ☐ Evidence handling and chain-of-custody procedures exist | Supports investigations, insurance claims, and potential legal/regulatory needs. | In Place / Partial / Not In Place |

## 5. Vulnerability and Change Management

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Vulnerability management covers critical IT assets | Scanning coverage, authentication, and prioritization are defined. | In Place / Partial / Not In Place |
| ☐ OT vulnerability approach respects uptime and safety constraints | Passive discovery, vendor coordination, and change windows are used. | In Place / Partial / Not In Place |
| ☐ Patch SLAs exist for critical vulnerabilities with governance for exceptions | Exceptions are approved with compensating controls and end dates. | In Place / Partial / Not In Place |
| ☐ End-of-life systems are tracked with a remediation plan | Migration plans or compensating controls reduce exposure for EOL assets. | In Place / Partial / Not In Place |
| ☐ Secure configuration drift is monitored and corrected | Baseline deviations are detected and remediated; configs are backed up. | In Place / Partial / Not In Place |
| ☐ Change management includes security review for impactful changes | Network, identity, and OT changes have defined approval and rollback steps. | In Place / Partial / Not In Place |
| ☐ External attack surface is monitored and reduced | Internet-facing assets are inventoried; unknown assets are discovered and remediated. | In Place / Partial / Not In Place |
| ☐ Penetration testing and validation simulate real adversary behavior | Testing targets perimeter, remote access, and high-impact service pathways. | In Place / Partial / Not In Place |

## 6. Backup, Recovery, and Continuity

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Backups cover critical systems, configs, and operational data | Includes network configs, OT engineering workstations, and key application data. | In Place / Partial / Not In Place |
| ☐ Immutable or offline backups are used where feasible | Reduces ransomware impact; backup accounts are separated and protected. | In Place / Partial / Not In Place |
| ☐ Backup health is monitored with defined remediation for failures | Alerting and ownership exist for backup job failures and storage issues. | In Place / Partial / Not In Place |
| ☐ Restore testing is performed and measured against RTO/RPO | Periodic restore drills validate recoverability of critical services. | In Place / Partial / Not In Place |
| ☐ Disaster recovery plans exist for key platforms and environments | DR plans include dependencies, sequencing, and validation steps. | In Place / Partial / Not In Place |
| ☐ Alternate communications channels are planned and tested | Out-of-band comms exist for major outages (e.g., phone trees, radios, secure chat). | In Place / Partial / Not In Place |
| ☐ Recovery requires approvals and includes safety validation | OT recovery includes operational safety checks before returning to service. | In Place / Partial / Not In Place |
| ☐ Post-incident recovery reviews drive improvements | After-action reviews update playbooks, architecture, and training. | In Place / Partial / Not In Place |

## 7. Third-Party and Supply Chain Resilience

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Vendor inventory includes access paths and criticality | Tracks vendor tools, credentials, remote access methods, and dependencies. | In Place / Partial / Not In Place |
| ☐ Contracts include enforceable security requirements | MFA, logging, patching, breach notification, and support SLAs are defined. | In Place / Partial / Not In Place |
| ☐ Security due diligence and ongoing monitoring are performed | Risk reviews are periodic and scaled to vendor criticality. | In Place / Partial / Not In Place |
| ☐ Remote support tools are approved, controlled, and monitored | Limits “shadow IT” remote access and ensures session accountability. | In Place / Partial / Not In Place |
| ☐ Vendor offboarding is prompt and verifiable | Accounts and credentials are removed; access paths are validated as closed. | In Place / Partial / Not In Place |
| ☐ Third-party incident coordination plan is documented | Defines roles, contacts, evidence sharing, and joint response expectations. | In Place / Partial / Not In Place |
| ☐ Contingency plan exists for vendor or cloud outages | Fallback options and escalation paths are defined for key providers. | In Place / Partial / Not In Place |
| ☐ Software supply chain risk is | Tracks critical components and update | In Place / Partial / |

| | | |
|---|---|---|
| considered for critical systems | mechanisms; monitors for compromise indicators. | Not In Place |

## 8. Training, Exercises, and Continuous Improvement

| Checklist item | What good looks like | Status / notes |
|---|---|---|
| ☐ Role-based training covers operators, engineers, and administrators | Training is tailored to duties (OT safety, incident reporting, secure operations). | In Place / Partial / Not In Place |
| ☐ Phishing and social engineering resilience is tested and improved | Managed phishing, training, and exception handling are documented. | In Place / Partial / Not In Place |
| ☐ Tabletop exercises are performed at least annually | Exercises include IT, OT, leadership, comms, and key vendors. | In Place / Partial / Not In Place |
| ☐ Technical recovery drills validate restore and failover procedures | Drills are measured and outcomes inform improvements. | In Place / Partial / Not In Place |
| ☐ After-action reports are tracked to closure | Findings have owners, due dates, and validation of completion. | In Place / Partial / Not In Place |
| ☐ Program reviews incorporate threat intel and lessons learned | Updates occur after incidents, major changes, and evolving threat patterns. | In Place / Partial / Not In Place |
| ☐ Quarterly metrics review informs roadmap and investment | Metrics drive prioritization of controls that reduce downtime risk. | In Place / Partial / Not In Place |
| ☐ Continuous improvement is embedded in SOPs and architecture | Playbooks, detection, segmentation, and backups evolve over time. | In Place / Partial / Not In Place |

## Selected Standards and References

This checklist is informed by widely used guidance for cyber resilience, operational technology security, incident response, and business continuity:

- CISA Cross-Sector Cybersecurity Performance Goals (CPG 2.0) (December 2025)
- NIST Cybersecurity Framework (CSF) 2.0 (February 2024)
- NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (2023)
- NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (2025)
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems (2010)
- NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems (2021)
- ISO 22301:2019 Business Continuity Management Systems

- ISO 22316:2017 Organizational Resilience - Principles and Attributes

Note: Sector-specific requirements (e.g., transportation, utilities, water, public sector) may impose additional expectations for reporting, testing, and controls. Organizations should identify applicable federal, state, and local requirements and align this checklist accordingly.

## How STIG Can Help

STIG helps critical infrastructure organizations improve operational resilience without disrupting uptime or safety-critical workflows. We focus on measurable outcomes—reduced downtime risk, faster recovery, and stronger governance—while aligning to widely recognized baselines such as CISA Cross-Sector Cybersecurity Performance Goals (CPG) and NIST CSF outcomes.

### What we do

- **Operational Resilience Assessment + Roadmap**
  Rapidly baseline your current state across governance, OT/IT segmentation, identity and remote access, monitoring, backup/recovery, and third-party exposure—then deliver a prioritized remediation plan tied to operational impact.
- **IT/OT Visibility and Segmentation Hardening**
  Improve asset inventory accuracy, define critical zones and trust boundaries, validate segmentation/OT DMZ design, and reduce lateral-movement pathways that drive broad outages.
- **Secure Remote Access and Privileged Control**
  Strengthen vendor and administrator access using MFA, least privilege, session accountability, and (where appropriate) privileged access management—without slowing operations teams down.
- **Detection, Response, and Downtime Playbooks**
  Operationalize monitoring and response expectations (including 24x7 options), build playbooks for high-impact scenarios (ransomware, remote access abuse, disruptive OT/IT incidents), and improve decision-making and escalation paths.
- **Backup, Recovery, and Continuity Validation**
  Design and validate recoverability for critical services—immutable backups where feasible,

restore testing against RTO/RPO, recovery sequencing, and safety checks before returning systems to service.

- **Third-Party Resilience and Supply Chain Risk**
  Inventory vendor access paths, define enforceable security requirements, implement ongoing oversight, and build contingency plans for vendor/cloud outages or compromise.
- **Exercises and Continuous Improvement**
  Run leadership and operator tabletop exercises, technical recovery drills, and after-action remediation tracking to close gaps and prove readiness.

## What you get

- A defensible **baseline scorecard** and gap list aligned to resilience outcomes
- A **prioritized roadmap** with owners, sequencing, and investment options
- **Artifacts** you can use for audits, insurer questionnaires, and executive reporting (e.g., evidence pack, diagrams, procedures, test results)

## Next Steps

1. **15–30 minute discovery call**
   Confirm your sector context, “must-not-fail” services, and top downtime scenarios (ransomware, vendor access, OT disruption, cloud/SaaS outage, etc.).
2. **Scope and data request (lightweight)**
   We’ll request a minimal set of inputs to accelerate results:
   - Critical services list (and known dependencies)
   - Network/identity architecture overview (even if high-level)
   - Current IR/BC/DR documentation (if available)
   - Vendor list with remote access methods
   - Any recent assessments, incidents, or outage postmortems
3. **Baseline Operational Resilience Review (2–4 weeks, typical)**
   STIG conducts stakeholder interviews and validates key technical and procedural controls, then produces:
   - Current-state maturity snapshot
   - Top risks and quick wins
   - 90-day stabilization plan + longer-term roadmap
   - Evidence pack outline and reporting artifacts
4. **Remediation execution options**
   Choose the implementation model that fits your constraints:

- **STIG-led** implementation with your teams (co-managed)
- **Hands-on engineering** for targeted initiatives (segmentation, logging, MFA/PAM, backup hardening)
- **Ongoing operational support** (monitoring, detection, response readiness, continuous testing)

5. **Validate and sustain**
   Schedule recurring exercises and recovery drills, refresh metrics quarterly, and update the roadmap after major changes—so resilience keeps pace with evolving threats and operational demands.