DURAND PORTER

STRATEGY. INNOVATION. IMPACT.

CYBERSECURITY COMPLIANCE & INCIDENT RESPONSE OPERATIONS MANUAL

Secure Operational Governance, Threat Response, and Regulatory Compliance Framework

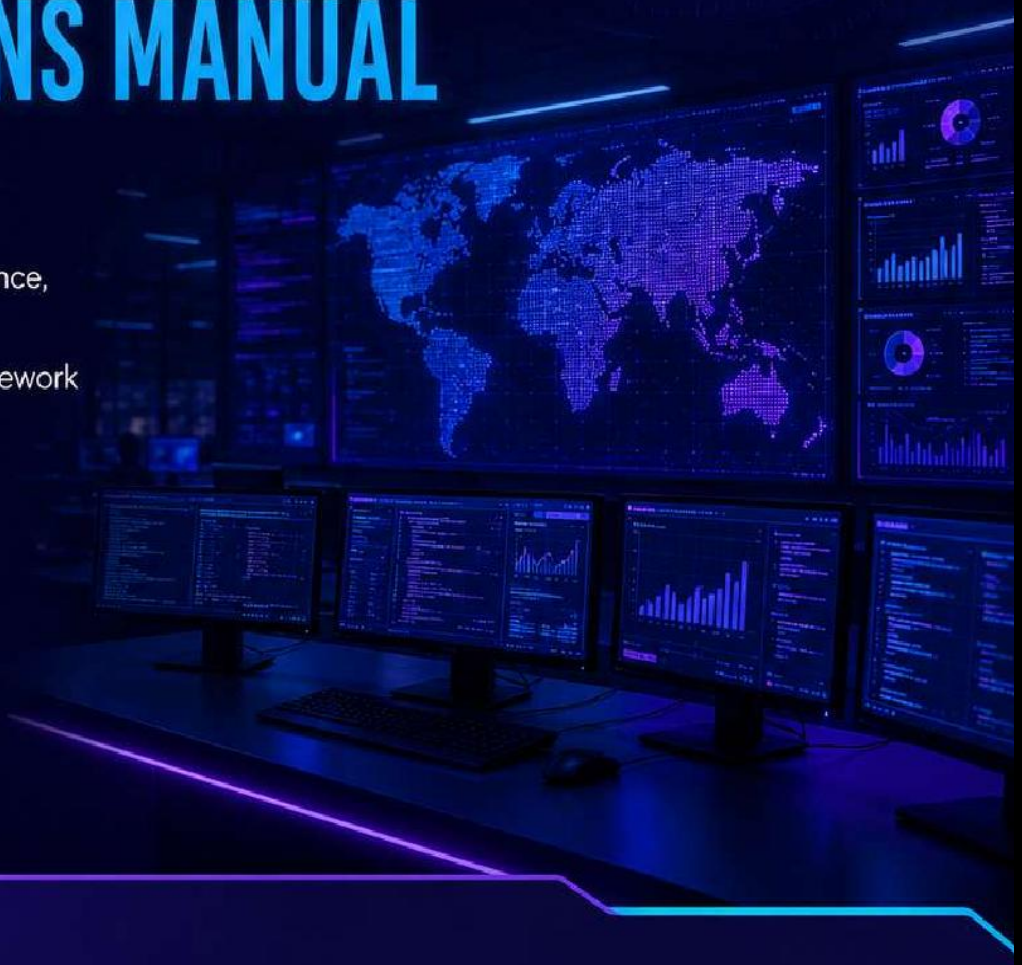

Table of Content

1. Executive Summary

This manual establishes enterprise cybersecurity governance, operational security standards, compliance controls, and incident response procedures required to protect organizational infrastructure, applications, cloud services, operational technology systems, and sensitive data assets.

This manual provides standardized operational guidance for:

- Security Operations Center (SOC) management
- Continuous security monitoring
- Threat detection and escalation
- Incident response coordination
- Vulnerability remediation
- Regulatory compliance management
- Business continuity operations
- Disaster recovery planning
- Digital forensics and evidence preservation

All cybersecurity operations shall align with the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, CIS Controls, SOC 2, HIPAA, GDPR, and PCI DSS compliance standards to support the organization's cybersecurity governance, operational resilience, and regulatory compliance objectives.

2. Governance & Compliance Framework

The organization shall maintain a formal cybersecurity governance structure to support enterprise-wide operational oversight, policy enforcement, risk management, and regulatory compliance activities. This governance structure establishes clear authority, accountability, and decision-making processes to ensure that cybersecurity objectives are aligned with organizational goals, regulatory obligations, and industry best practices. Governance activities shall support the effective implementation, monitoring, and continuous improvement of the organization's cybersecurity program.

The Cybersecurity Steering Committee is responsible for providing strategic oversight of the organization's cybersecurity program and ensuring that security initiatives remain aligned with business objectives and compliance requirements. The committee shall periodically review cybersecurity performance, evaluate enterprise risks, and provide direction for security policies and operational priorities.

The Cybersecurity Steering Committee is responsible for:

- Enterprise security governance
- Policy approval and review
- Cybersecurity budget oversight
- Risk management direction
- Executive-level reporting

The Chief Information Security Officer (CISO) maintains overall accountability for cybersecurity operations, compliance readiness, and incident escalation management. The CISO provides executive leadership for the cybersecurity program, oversees the implementation of security policies and standards, coordinates enterprise security initiatives, and ensures that significant cybersecurity risks and incidents are communicated to executive management in a timely manner.

Compliance reviews shall occur quarterly to evaluate the effectiveness of cybersecurity controls, verify adherence to organizational policies, identify compliance gaps, and ensure ongoing alignment with applicable regulatory and industry requirements. Review results shall be documented and used to support continuous improvement of the organization's cybersecurity governance and compliance program.

Compliance reviews shall occur quarterly and include:

- Policy validation
- Access control audits
- SIEM log review
- Regulatory gap analysis
- Third-party risk assessments

3. Security Operations Center Procedures

The Security Operations Center (SOC) shall operate continuously to monitor enterprise infrastructure, identify suspicious activity, and coordinate incident response operations. The SOC serves as the central function for enterprise security monitoring, providing continuous visibility into the organization's information systems, networks, cloud environments, and security events. Through proactive monitoring and timely response, the SOC supports the identification, investigation, containment, and escalation of potential cybersecurity threats to minimize operational and business risk.

The SOC shall operate using a tiered support model to ensure the efficient handling, investigation, and escalation of security events based on their complexity and potential impact.

SOC Tier Structure:

Tier 1 – Security alert monitoring and triage

Tier 2 – Incident investigation and correlation

Tier 3 – Advanced threat analysis and containment

SOC analysts shall continuously monitor enterprise security events and activities to identify indicators of compromise, suspicious behavior, and potential policy violations. Monitoring activities shall include, but are not be limited to:

- Authentication events
- Privileged account activity
- Malware detections
- Endpoint alerts
- Data transfer anomalies
- Cloud security events
- Network intrusion attempts

Critical incidents shall be escalated to the Incident Response Manager within fifteen (15) minutes of detection to ensure timely assessment, containment, and coordination of response activities in accordance with the organization's incident response procedures.

4. Incident Response Operations

The organization shall maintain a formal incident response lifecycle consisting of defined processes and procedures for identifying, managing, and recovering from cybersecurity incidents. The incident response lifecycle provides a structured approach for minimizing operational disruption, reducing the impact of security events, preserving critical evidence, and restoring affected systems in a timely and controlled manner.

The incident response lifecycle shall consist of:

1. **Preparation** – Establish and maintain the policies, procedures, tools, communication plans, and resources necessary to effectively respond to cybersecurity incidents.
2. **Identification** – Detect, analyze, and validate suspected cybersecurity incidents to determine their nature, scope, severity, and potential impact on organizational operations.
3. **Containment** – Implement appropriate measures to isolate affected systems, limit the spread of the incident, and prevent further compromise while preserving evidence.
4. **Eradication** – Remove malicious code, unauthorized access, vulnerabilities, or other threats from affected systems to eliminate the root cause of the incident.
5. **Recovery** – Restore affected systems, applications, and services to normal operational status after validating system integrity and confirming that security controls are functioning as intended.
6. **Lessons Learned** – Conduct a post-incident review to document findings, evaluate the effectiveness of the response, identify improvement opportunities, and update policies, procedures, or security controls as necessary.

Containment procedures shall be implemented to limit the spread and impact of confirmed or suspected cybersecurity incidents while preserving the integrity of affected systems and supporting subsequent investigation activities. Containment procedures may include:

- **Isolation of compromised endpoints** – Disconnect affected devices from the network to prevent further unauthorized access or malware propagation.
- **Suspension of privileged accounts** – Temporarily disable privileged accounts suspected of compromise to prevent unauthorized administrative activities.

- **Blocking malicious IP addresses** – Restrict network communications originating from or directed to known malicious IP addresses to reduce the risk of continued attacks.
- **Segmentation of affected networks** – Isolate impacted network segments to contain the incident and prevent lateral movement across the enterprise environment.
- **Preservation of forensic evidence** – Secure and maintain system logs, memory captures, and other digital evidence to support incident investigation, legal proceedings, and regulatory requirements.

Recovery activities shall validate system integrity prior to restoring production operations. Validation shall confirm that affected systems have been remediated, verified, and are operating as intended before normal business operations resume.

All incident investigations must maintain documented chain-of-custody procedures for forensic evidence handling. Chain-of-custody documentation shall ensure that evidence is collected, preserved, transferred, and stored in a manner that maintains its integrity and supports investigative, legal, and regulatory requirements.

5. Vulnerability Management Procedures

The organization shall maintain a formal vulnerability management program to identify, assess, prioritize, remediate, and monitor security vulnerabilities across enterprise systems, applications, networks, cloud environments, and supporting infrastructure. The program shall support proactive risk reduction by ensuring that identified vulnerabilities are addressed in accordance with established remediation priorities and organizational security requirements.

The vulnerability management program shall include:

- **Automated vulnerability scanning** – Perform automated scans to identify known vulnerabilities, security weaknesses, and configuration issues across enterprise assets.
- **Risk prioritization** – Assess identified vulnerabilities based on their severity, potential impact, exploitability, and associated business risk to determine remediation priorities.
- **Patch validation** – Verify that security patches and updates have been successfully applied and that systems continue to operate as intended following implementation.
- **Remediation tracking** – Monitor and document the status of vulnerability remediation activities to ensure timely resolution and accountability.
- **Compliance reporting** – Generate reports that demonstrate compliance with organizational policies, regulatory requirements, and applicable security standards.

Scanning Frequency

Vulnerability assessments shall be performed according to the following schedule to maintain continuous visibility into the organization's security posture:

- **Internet-facing systems – Weekly:** Conduct weekly vulnerability scans on publicly accessible systems to identify and remediate externally exposed security risks.
- **Internal infrastructure – Monthly:** Perform monthly scans of internal systems and network infrastructure to detect vulnerabilities within the enterprise environment.
- **Cloud environments – Continuous:** Continuously monitor cloud resources for newly identified vulnerabilities, configuration changes, and emerging security risks.

- **Critical infrastructure – Daily monitoring:** Monitor critical infrastructure daily to rapidly identify vulnerabilities that may significantly impact business operations or essential services.

Patch Remediation Standards

Identified vulnerabilities shall be remediated according to the following timeframes based on their assigned severity:

- **Critical:** 24 Hours
- **High:** 72 Hours
- **Medium:** 14 Days
- **Low:** 30 Days

Unpatched critical vulnerabilities require executive escalation to ensure appropriate risk management decisions, resource allocation, and timely remediation actions are implemented.

6. Identity & Access Management

The organization shall enforce strict identity and access management controls to prevent unauthorized access to enterprise systems and data assets. These controls shall ensure that users are granted appropriate access based on their roles and responsibilities while protecting sensitive information from unauthorized use or disclosure.

Required controls include:

- **Multi-factor authentication (MFA)** – Require multiple forms of identity verification before granting system access.
- **Role-based access control (RBAC)** – Assign system access based on job roles and business responsibilities.
- **Least privilege enforcement** – Limit user access to only the permissions necessary to perform assigned duties.
- **Privileged access monitoring** – Monitor privileged accounts to detect unauthorized or suspicious activities.
- **Password complexity requirements** – Enforce strong password standards to enhance account security.
- **Quarterly access reviews** – Review user access permissions every quarter to ensure continued authorization.

Privileged accounts shall require:

- **Formal approval** – Obtain management authorization before privileged access is granted.
- **Security monitoring** – Continuously monitor privileged account activities for security events.
- **Session logging** – Record privileged sessions to support auditing and investigations.
- **Periodic review and recertification** – Regularly review and validate privileged access to ensure it remains appropriate.

Access violations shall trigger immediate SOC investigation procedures to determine the cause, assess potential security risks, and initiate appropriate response actions.

7. Network & Endpoint Security Standards

The network security architecture shall implement layered security controls to protect enterprise networks, systems, and communications from unauthorized access, cyber threats, and malicious activities.

The network security architecture shall implement:

- **Firewalls** – Filter and control inbound and outbound network traffic based on approved security rules.
- **IDS/IPS technologies** – Detect and prevent unauthorized or malicious network activity.
- **Secure VPN access** – Provide encrypted remote access for authorized users.
- **Network segmentation** – Separate network environments to limit unauthorized access and reduce the spread of security incidents.
- **Encrypted communications** – Protect data transmitted across networks through encryption.
- **Continuous traffic inspection** – Monitor network traffic to identify suspicious activities and potential security threats.

Endpoint protection requirements include:

- **Endpoint Detection & Response (EDR)** – Continuously monitor endpoints to detect, investigate, and respond to security threats.
- **Anti-malware protection** – Detect, prevent, and remove malicious software from endpoint devices.
- **Device encryption** – Encrypt endpoint data to protect information from unauthorized access.
- **USB restriction policies** – Control the use of removable media to reduce the risk of malware infection and data loss.
- **Secure configuration baselines** – Maintain standardized and secure system configurations across endpoint devices.

Firewall rule reviews shall occur quarterly and follow deny-by-default security standards to ensure that only authorized network traffic is permitted and unnecessary access is removed.

8. Threat Intelligence & Monitoring

Threat intelligence operations shall support proactive defense capabilities through continuous monitoring of emerging cybersecurity threats and adversary activity. These operations shall enable the organization to identify, assess, and respond to potential threats by leveraging timely and relevant threat intelligence to strengthen security monitoring and incident response activities.

Threat intelligence sources include:

- **Government advisories** – Provide official cybersecurity alerts, threat information, and security recommendations issued by government agencies.
- **Commercial intelligence feeds** – Supply current threat intelligence, indicators of compromise (IOCs), and information on emerging cyber threats from trusted providers.
- **Internal incident reports** – Utilize information from previous security incidents to identify trends, recurring threats, and opportunities for improving security controls.
- **ISAC intelligence sources** – Obtain industry-specific threat intelligence and best practices through Information Sharing and Analysis Centers (ISACs).

Threat intelligence activities include:

- **Indicator correlation** – Analyze and correlate indicators of compromise across multiple security events and data sources.
- **Threat hunting** – Proactively search enterprise systems and networks for signs of malicious activity that may have bypassed existing security controls.
- **Adversary analysis** – Evaluate attacker tactics, techniques, and procedures (TTPs) to improve threat detection and defensive capabilities.
- **Detection rule development** – Develop and refine security monitoring rules to improve the identification of malicious activities.
- **Malware analysis support** – Assist in the analysis of malicious software to understand its behavior, impact, and recommended mitigation measures.

The Security Information and Event Management (SIEM) platform shall aggregate enterprise security logs and generate automated alert escalation workflows to support continuous monitoring, threat detection, incident investigation, and timely response.

9. Business Continuity & Disaster Recovery

The organization shall maintain documented disaster recovery and business continuity procedures to support operational resilience during disruptive cybersecurity events. These procedures shall establish the processes required to restore critical systems, recover data, and resume business operations while minimizing downtime and operational impact.

Recovery Objectives

- **Recovery Time Objective (RTO): 4 Hours** – The maximum acceptable time to restore critical systems and services following a disruption.
- **Recovery Point Objective (RPO): 1 Hour** – The maximum acceptable amount of data loss measured by the time between the last recoverable backup and the disruption.

Disaster Recovery Procedures

Disaster recovery procedures include:

- **Secure backup validation** – Verify that backup data is complete, secure, and available for system recovery.

- **Recovery testing** – Perform regular testing to confirm that recovery procedures are effective and operational.
- **Infrastructure failover procedures** – Transfer critical operations to alternate infrastructure during system outages or disruptions.
- **Restoration integrity checks** – Validate the integrity and functionality of restored systems before returning them to production.
- **Emergency communications** – Coordinate timely communication with stakeholders during disaster recovery activities.

Disaster recovery exercises shall occur semi-annually and following major infrastructure modifications to validate recovery procedures, confirm operational readiness, and identify opportunities for continuous improvement.

10. Audit & Compliance Procedures

The organization shall conduct internal and external audit activities to evaluate the effectiveness of cybersecurity controls, verify compliance with organizational policies and applicable regulatory requirements, and identify opportunities for continuous improvement.

Internal audit reviews shall validate:

- **Security policy compliance** – Verify that cybersecurity policies and procedures are implemented and followed throughout the organization.
- **Access control enforcement** – Confirm that user access permissions are appropriately assigned, managed, and enforced.
- **Incident response readiness** – Assess the organization's preparedness to detect, respond to, and recover from cybersecurity incidents.
- **Vulnerability remediation tracking** – Verify that identified vulnerabilities are remediated within established timeframes and properly documented.
- **Backup validation procedures** – Confirm that backup processes are functioning effectively and support successful data recovery.
- **Logging and monitoring controls** – Evaluate the effectiveness of logging, monitoring, and alerting capabilities for detecting security events.

External assessments may include:

- **Penetration testing** – Simulate cyberattacks to identify exploitable vulnerabilities within the organization's environment.
- **Red team exercises** – Conduct controlled adversary simulations to evaluate the effectiveness of security controls and incident response capabilities.
- **Regulatory audits** – Assess compliance with applicable laws, regulations, and industry standards.
- **Third-party security reviews** – Evaluate the effectiveness of cybersecurity controls through independent security assessments.

Audit findings shall be documented, tracked, and remediated according to established compliance timelines. Corrective actions shall be monitored through completion to ensure identified issues are resolved and compliance objectives are achieve.

Conclusion

This Enterprise Cybersecurity Operations Manual establishes the governance framework, operational procedures, and security controls required to protect the organization's information systems, infrastructure, cloud services, operational technology systems, and sensitive data assets. The policies, standards, and procedures contained in this manual provide a consistent approach to managing cybersecurity risks, supporting regulatory compliance, and maintaining the confidentiality, integrity, and availability of organizational information and critical business resources.

The successful implementation of this manual requires the commitment and cooperation of executive management, business units, information technology personnel, cybersecurity teams, and all authorized users. Each individual with assigned cybersecurity responsibilities shall comply with the policies and operational requirements outlined in this manual to support the organization's overall security posture and reduce the risk of cybersecurity incidents.

Cybersecurity is a continuous process that requires ongoing monitoring, assessment, and improvement to address evolving threats, emerging technologies, and changing regulatory requirements. The organization shall periodically review and update this manual to ensure that its policies, procedures, and security controls remain effective, relevant, and aligned with organizational objectives, applicable laws, industry standards, and recognized cybersecurity frameworks.

Compliance with the requirements contained in this manual supports effective cybersecurity governance, operational resilience, incident preparedness, business continuity, and continuous improvement. Through the consistent application of these requirements, the organization strengthens its ability to prevent, detect, respond to, and recover from cybersecurity incidents while protecting critical systems, business operations, and information assets.

Operational Appendices

The appendices provide supporting documentation, reference materials, templates, and operational checklists that complement the policies and procedures outlined in this manual. These resources are intended to promote consistency, support incident response and recovery activities, facilitate compliance efforts, and assist personnel in performing cybersecurity operations effectively.

Appendices shall include:

- **Incident Severity Matrix** – Defines incident severity levels and the corresponding response priorities and escalation requirements.
- **Incident Response Checklist** – Provides a step-by-step checklist to guide personnel through the incident response process.
- **Escalation Matrix** – Identifies escalation procedures, responsible personnel, and communication paths for security incidents.
- **Evidence Chain-of-Custody Form** – Documents the collection, handling, transfer, and storage of forensic evidence to preserve its integrity.
- **Disaster Recovery Validation Checklist** – Verifies that recovery procedures have been completed successfully before systems are returned to production.
- **Compliance Mapping Matrix** – Maps organizational cybersecurity controls to applicable regulatory and industry compliance requirements.
- **Security Audit Checklist** – Provides a standardized checklist for conducting internal security audits and compliance reviews.
- **Ransomware Response Procedures** – Establishes procedures for identifying, containing, responding to, and recovering from ransomware incidents.

Appendix A - Incident Severity Matrix

Severity	Impact	Response Time	Escalation
Critical	Enterprise-wide compromise	Immediate	Executive Leadership
High	Major operational disruption	< 1 Hour	CISO
Medium	Limited operational impact	< 4 Hours	SOC Manager
Low	Minor operational impact	< 24 Hours	Operations Team

DURAND PORTER

STRATEGY. INNOVATION. IMPACT.

THANK YOU

We appreciate the opportunity to partner on this critical mission. Together, we can drive innovation, enhance system capabilities, and build a more resilient future for aerospace.

Salt Lake City, UT, US, 84107

durandmporter@gmail.com

+1 8056378355