OSTENDIO

CHECKLIST

The InfoSec Playbook for Serious Security Pros

This InfoSec activity checklist is crafted by serious security professionals for serious security professionals. Within this checklist, you'll find annual, quarterly, monthly and daily information security tasks that will help you and your people practice continuous security. Reference this checklist whenever you need a guide to keep your team on track, remediate gaps in your security program, or meet specific framework standards.

ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Annual meeting of the Information Security Management Committee: 1. Review of security policies and procedures (high-level) 2. Risk assessment and management 3. Cybersecurity best practices 4. Security awareness and training initiatives 5. Disaster recovery and business continuity planning 6. Security audit and compliance status 7. Implementation of new security solutions 8. Security incident response and management 9. Security monitoring and reporting 10. Budget and resource allocation 11. Collaboration with external partners and vendors 12. Regulatory and legal compliance updates	ISMC	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	ISMC Members might include: CTO ISO VP, Engineering Director of IT Director, People Operations Associate General Counsel
Test & Update the Business Continutiy Plan: Outline how the business will continue to operatate in the event of a disruption.	Executive Leadership, IT Personnel, Internal Auditors, Business Personnel, Third Party Consultants	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	

ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Perform a Business Impact Analysis: Identify and evaluate the potential effects of a disruption to the organization's operations.	Executive Leadership, IT Personnel, Internal Auditors, Business Personnel, Third Party Consultants	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	
Perform a Risk Assessment: Identify potential areas of vulnerability, update security policies and procedures, and review existing security controls.	Executive Leadership, IT Personnel, Internal Auditors, Business Personnel, Third Party Consultants	AICPA TSP 100 HIPAA Security Rule HITRUST ISO 27001:2017 NIST 800-53	
Test Backup and Disaster Recovery Plans: Ensure that all backup and disaster recovery plans are up to date and can be implemented in the event of an emergency.	Executive Leadership, IT Personnel, Internal Auditors, End Users, Third Party Consultants	AICPA TSP 100 HIPAA Security Rule HITRUST ISO 27001:2017 NIST 800-53	
Conduct Penetration Testing: Test the organization's systems to identify any potential weaknesses.	ISO / InfoSec Team	AICPA TSP 100 HIPAA Security Rule HITRUST ISO 27001:2017 NIST 800-53	
SOC 2 Type II Audit / Independent review of the ISMP.	Executive Leadership, IT Personnel, Internal Auditors, Business Personnel, Third Party Consultants	AICPA TSP 100 HITRUST NIST 800-53 ISO 27001:2017	

ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Review & update Disciplinary Policy Factors to consider: - Consistency and Fairness: Is it fair and consistent across the organization? - Clarity: Is it clearly written and easy to understand? - Transparency: Is the policy transparent and communicated effectively to all employees? - Reasonableness: Are the potential actions outlined reasonable and appropriate for the offense? - Legality: Is the policy compliant with relevant laws and regulations? - Effectiveness: Is the policy effective at addressing and preventing policy violations? - Support: Does the policy provide support for personnel who might need help addressing the underlying issues that may have led to their policy violation?	HR, CTO, ISMC	HITRUST NIST 800-53 ISO 27001:2017 HIPAA Security Rule	
Review and update Information Security Management Program (ISMP) Policies and Procedures Factors to consider: - Changes to the operating environment - Change in relevant laws and regulations - Feedback from the workforce - Changes in the threat landscape - Alignment with the chosen information security framework - Effectiveness of the current policies and procedures	ISMC, ISO, CTO	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	Some information security frameworks require organizations to review and update the information security policies and procedures at least annually.
After an annual update of the ISMP: Annual acknowledgement of ISMP Policies and Procedures by workforce personnel	HR, ISMC	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	
Data assets inventory review: - Identify the data assets - structured/unstructured, databases, files and documents - Catalog the data assets - Identify characteristics (type, format, location) - Analyze the data assets - How are they being used? - Document the findings	Engineering IT Team, InfoSec	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	Know where your sensitive data lives.

ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Physical assets inventory review (workstations, laptops, servers, networking components, etc) The device inventories should be updated regularly and any changes should be documented. Verify asset inventories are not duplicated.	Engineering IT Team, InfoSec	AICPA TSP 100 HITRUST ISO 27001:2017 NIST 800-53	
Review Software Development Lifecycle and Secure Coding Guidelines – Review the SDLC and secure coding guidelines vs. changes that may have occured in industry standards, the organizations goals and priorities, technology or infrastructure, compliance requirements, or risk profile. – Verify compliance with the software development process and industry standards – Document the findings	Engineering	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Review third-party agreements & SLA's – Identify the thrid-party agreements and SLA's – Review the terms and conditions of the agreements – Verify the adequacy of the information security protections – Document the findings	CTO, ISMC, Counsel	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	AWS, Google Cloud, Azure, etc Critical SaaS solutions used by the org
Review and update Acceptable Use Policy – Review the policy against relevant laws and regulations such as the Computer Fraud & Abuse Act – Verify the effectiveness of the policy in protecting the organization's information systems, networks and resources – Document the findings	ISMC, HR	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	Done at annual ISMC meeting (item 1)
Annual Access Rights Acknowledgement (Acceptable Use Policy)	HR	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	All personnel acknowledge annually
Review of SIEM tools being used and data being used; Confirm legal requirements regarding monitoring authorized access are met.	InfoSec, IT Team, Engineering, Legal Counsel	HITRUST NIST 800-53	From a legal perspective this would also apply to any monitoring done on endpoints via Endpoint Management Tools or Email (i.e., workforce activity monitoring)

ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Security Awareness Training: Train employees on the latest security best practices and ensure they are aware of how to protect the organization from threats.	HR	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Training personnel on the Incidence Response Plan – Identify the audience such as IT Staff, InfoSec Team and Management – Review the plan to ensure it is up-to-date – Develop a training program that covers key elements of the plan – Conduct the training – Evaluate the effectiveness of the training	ISMC	AICPA TSP 100 HIPAA HITRUST NIST 800-53	For personnel with responsibilities in these areas.
Insider Threat Training	HR	HIPAA HITRUST ISO 27001:2017 NIST 800-53	KnowBe4; for ISMC and senior management (CTO, HR, IT, Engineering)
Review Data Classification Policy and controls – Review the policy against current / relevant laws and regulations such as HIPAA and GDPR – Verify the effectiveness of the policy – Document the findings	ISMC	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	Do this at the annual ISMC meeting (item 1)
Review the privacy policy – Review the policy against relevant laws and regulations such as HIPAA, GDPR, CCPA – Verify the effectiveness of the policy – Ensure that individuals are able to contact the organzations privacy officer – Document the findings	Legal Counsel	HIPAA HITRUST ISO 27001:2017 NIST 800-53	

BI-ANNUALLY

Description	Responsibility	InfoSec Framework	Comments
Review secure configuration/hardening standards for user endpoints	IT Team, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Review secure configuration/hardening standards for production environment	Engineering, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

QUARTERLY

Description	Responsibility	InfoSec Framework	Comments
Perform Vulnerability Assessments: Identify and address any potential vulnerabilities in the system, including patch management and configuration management	InfoSec Team	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Check for unauthorized mobile devices on the network. This can be accomplished through: - Network Scanning - Access Point Monitoring - Network Traffic Analysis - Mobile Device Management - Physical Inspections	Engineering, IT Team, ISMC, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

QUARTERLY

Description	Responsibility	InfoSec Framework	Comments
Check for rogue wireless networks. Use a wireless scanner or other tools to check for wireless networks that are present in the environment. – If an unauthorized AWP is found: – Disconnect the device – File an incident ticket to investigate – Determine if sensitive data has been stolen – Implement additinonal security measures	IT Team, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Perform an audit of the execution of privileged activities on systems. – Identify privileged activities – Review logs and records of privileged activities – verify the appropriateness of privileged activites – Document the findings	IT Team Engineering, InfoSec	HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Physical security compliance review. This might include: – Review of visitor logs – Review of badge access control logs – Review of security equipment (door locks, cameras, alarm systems) – Document findings and take corrective actions as needed.	ISO, InfoSec Team, Facilities Mgt	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Review Non-Privileged User Access Rights: Ensure that access rights are current and that users only have access to the data and systems they need to do their jobs.	IT Team Engineering, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

EVERY 60 DAYS

Description	Responsibility	InfoSec Framework	Comments
Review Privileged User Access Rights: Ensure that access rights are current and that users only have access to the data and systems they need to do their jobs.	IT Team Engineering, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

MONTHLY

Description	Responsibility	InfoSec Framework	Comments
Information Security Management Committee Meeting (ISMC). Agenda items may include: – Review of current threats and vulnerabiliies - As identified through CISA alerts, vulnerability scans or penetration tests – Changes to security policies or procedures – Security and awareness training initiatives such as phishing tests, etc. – Compliance issues related to laws or regulations – Review of any recent security incidents – Review of any insider threat risks such as pending terminations, etc.	ISMC	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

DAILY

Description	Responsibility	InfoSec Framework	Comments
Review of system alerts, events and activities – Set up alerts and notifications – Review the logs and alerts daily – Analyze and investigate suspicious activity – Document and report on findings – Follow up on outstanding issues	InfoSec Team IT Team	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Monitor Network Traffic: Monitor inbound and outbound traffic to detect any suspicious activity. Network analysis tools - AWS VPC Flow Logs, Azure Network Watcher or Google Cloud Network Insights Intrusion Detection Systems - AWS Guard Duty, AWS WAF, Azure Security Center, GCP Security Command Center	IT Team Engineering, InfoSec	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	
Monitor system performance and capacity AWS CloudWatch, Azure Monitor, GCP Stack Driver, Autoscalling Tools	IT Team	AICPA TSP 100 HIPAA HITRUST ISO 27001:2017 NIST 800-53	

Everyone Secure.

Welcome to the next generation of security.

Ostendio is the only security and risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

Schedule a demo today.

HITRUST Authorized Readiness Licensee