Questionnaire

Friday, January 10, 2025 2:43 PM

Section 1: Multi-Factor Authentication (MFA)

1.1 Is MFA enforced for all privileged accounts and remote access systems?
1.2 Are phishing-resistant MFA methods (e.g., hardware tokens, FIDO2 keys) deployed?
1.3 Are MFA logs monitored for anomalies and failed attempts?
1.4 Are MFA requirements integrated into all new systems before deployment?
1.5 How often is MFA effectiveness tested (e.g., phishing simulations)?

Section 2: Backup and Recovery

2.1 Are backups configured to be immutable (e.g., WORM storage) and segregated from the primary network?
2.2 Are backup restoration processes tested at least quarterly?
2.3 Are unauthorized backup access attempts logged and alerted?
2.4 Is there a documented backup retention policy aligned with business requirements?
2.5 Are critical system backups included in simulated ransomware recovery scenarios?

Section 3: Endpoint Detection and Response (EDR)

3.1 Is an EDR solution deployed across all endpoints, including servers?
3.2 Does the EDR detect and block unauthorized tools (e.g., certutil.exe, rclone.exe)?
3.3 Are EDR policies reviewed and updated regularly to address emerging threats?
3.4 Are alerts from the EDR system integrated with incident response processes?
3.5 Are simulated attacks conducted to test the EDR's effectiveness?

Section 4: Logging and Monitoring

4.1 Is a SIEM system deployed for centralized log management and analysis?
4.2 Are logs configured to capture critical events (e.g., privilege escalation, lateral movement)?
4.3 Are log retention policies aligned with regulatory requirements?
4.4 Are logs reviewed regularly for anomalies, and findings reported?
4.5 Are alert thresholds validated and tested for effectiveness?

Section 5: Incident Response and Recovery

5.1 Is there a documented Incident Response Plan (IRP), and is it reviewed annually?
5.2 Are regular incident response drills conducted, including ransomware scenarios?
5.3 Are roles and responsibilities within the IRP clearly defined?
5.4 Are lessons learned from incidents incorporated into the IRP?
5.5 Are post-incident reviews documented and shared with stakeholders?

Section 6: Network and Endpoint Security

6.1 Is network segmentation implemented to isolate critical resources (e.g., databases,

backups)?
6.2 Are inter-zone communications restricted using firewalls or NAC?
6.3 Are unused ports, protocols, and services disabled on all systems?
6.4 Are firewalls, IDS/IPS, and endpoint protections updated regularly?
6.5 Are anomaly detection systems in place to monitor network traffic?

Section 7: Privileged Access Management

7.1 Is privileged access protected by MFA and restricted to authorized roles?
7.2 Are privileged account activities monitored and logged for review?
7.3 Are Just-In-Time (JIT) access policies enforced for administrative tasks?
7.4 Are privileged accounts reviewed quarterly for appropriateness of access?
7.5 Is there a process for revoking access immediately upon termination or role change?

Section 8: Security Awareness and Training

8.1 Is annual security awareness training conducted for all employees?
8.2 Are phishing simulations conducted to test employee readiness?
8.3 Are training materials updated to address new threats?
8.4 Are training results tracked to identify high-risk areas?
8.5 Is additional training provided for employees who fail phishing tests?

Section 9: Change and Configuration Management

9.1 Is there a documented change management policy, including CAB approval?
9.2 Are system configurations reviewed quarterly for deviations from baselines?
9.3 Are all configuration changes tested, validated, and documented before deployment?
9.4 Are rollback procedures included in configuration management plans?
9.5 Are automated tools used to enforce configuration standards?

Section 10: Data Protection and DLP

10.1 Is a DLP solution deployed to monitor and block unauthorized data transfers?
10.2 Are sensitive data repositories restricted to authorized users?
10.3 Are data transfer tools (e.g., rclone.exe) restricted or monitored?
10.4 Are DLP policies tested for effectiveness through simulated exfiltration attempts?
10.5 Are employees trained on secure data handling policies?

Section 11: Testing and Continuous Improvement

11.1 Are vulnerability scans conducted on all systems at least quarterly?
11.2 Is penetration testing performed to identify and mitigate weaknesses?
11.3 Are corrective actions from tests tracked and verified for effectiveness?
11.4 Are testing results reported to senior management and the board?
11.5 Is the testing schedule updated to reflect emerging threats?

Section 12: Compliance and Audit

12.1 Are periodic audits conducted to evaluate security controls and compliance?
12.2 Are audit findings documented, and remediation plans tracked?
12.3 Are audit logs preserved for forensic analysis for at least 12 months?
12.4 Are board-level reports prepared on security program status and incidents?
12.5 Are independent reviews conducted to validate control effectiveness?

Section 13: Vendor and Third-Party Management

13.1 Are vendors required to comply with the institution's security policies?
13.2 Are due diligence and risk assessments conducted for all third-party relationships?
13.3 Are third-party access and activities monitored for compliance?
13.4 Are incident response capabilities of third parties reviewed periodically?
13.5 Is vendor access promptly removed upon contract termination?

Section 1: Multi-Factor Authentication (MFA)

1.1 **Is MFA enforced for all privileged accounts and remote access systems?**

- **What to provide:** Documentation of MFA enforcement policies, screenshots of MFA configurations in systems (e.g., Active Directory, VPN), and audit logs verifying MFA usage.
- **Example:** A screenshot from your VPN configuration tool showing MFA setup or policy documentation specifying MFA requirements for all privileged accounts.

1.2 **Are phishing-resistant MFA methods (e.g., hardware tokens, FIDO2 keys) deployed?**

- **What to provide:** A list of MFA methods implemented, proof of deployment (e.g., hardware token serial numbers), and configuration screenshots.
- **Example:** Details of hardware tokens issued to administrators or screenshots showing the use of an authenticator app with phishing-resistant protocols.

1.3 **Are MFA logs monitored for anomalies and failed attempts?**

- **What to provide:** Examples of logs showing successful and failed attempts, details of the monitoring process, and reports of any incidents detected through MFA logs.
- **Example:** A security dashboard screenshot showing failed MFA attempts and corresponding alerts.

1.4 **Are MFA requirements integrated into all new systems before deployment?**

- **What to provide:** Documentation outlining the deployment process for new systems and integration of MFA, including testing results.
- **Example:** A project checklist showing MFA activation as a required step during deployment.

1.5 **How often is MFA effectiveness tested (e.g., phishing simulations)?**

- **What to provide:** Test schedules, reports of phishing simulations or other testing exercises, and examples of corrective actions taken.
- **Example:** Results from a phishing simulation exercise showing MFA prevented unauthorized access.

Section 2: Backup and Recovery

2.1 **Are backups configured to be immutable (e.g., WORM storage) and**

segregated from the primary network?

- **What to provide:** Architecture diagrams, configuration screenshots of backup systems, and storage provider contracts.
- **Example:** A diagram showing air-gapped backups or screenshots of a WORM storage configuration.

2.2 **Are backup restoration processes tested at least quarterly?**

- **What to provide:** Test schedules, test logs, and evidence of test results, including any corrective actions.
- **Example:** A report from the latest quarterly restoration test showing recovery times and success metrics.

2.3 **Are unauthorized backup access attempts logged and alerted?**

- **What to provide:** Backup system logs, alerting configurations, and incident reports if any unauthorized access was detected.
- **Example:** A log entry showing an attempted unauthorized access and an alert triggered in the monitoring system.

2.4 **Is there a documented backup retention policy aligned with business requirements?**

- **What to provide:** The backup retention policy document and examples of how retention is enforced (e.g., automated deletion schedules).
- **Example:** A policy specifying a 7-year retention period for regulatory compliance.

2.5 **Are critical system backups included in simulated ransomware recovery scenarios?**

- **What to provide:** Evidence of ransomware recovery testing, including test scripts and results showing recovery success.
- **Example:** A scenario-based recovery test report validating the restoration of critical systems.

Section 3: Endpoint Detection and Response (EDR)

3.1 **Is an EDR solution deployed across all endpoints, including servers?**

- **What to provide:** Deployment logs, screenshots of EDR software dashboards, and lists of endpoints covered.
- **Example:** A screenshot from the EDR console showing all servers and workstations being monitored.

3.2 **Does the EDR detect and block unauthorized tools (e.g., certutil.exe, rclone.exe)?**

- **What to provide:** Evidence of blocked attempts, policy configurations, and testing results for unauthorized tool detection.
- **Example:** A log entry from the EDR solution showing a blocked attempt to execute rclone.exe.

3.3 **Are EDR policies reviewed and updated regularly to address emerging threats?**

- **What to provide:** Change logs for EDR policies, review schedules, and documentation of updates.
- **Example:** A record of a policy update to address a new malware variant.

3.4 **Are alerts from the EDR system integrated with incident response processes?**

- **What to provide:** Incident response procedures, integration documentation, and examples of alerts leading to response actions.
- **Example:** An incident report showing how an EDR alert triggered containment

actions.

3.5 **Are simulated attacks conducted to test the EDR's effectiveness?**

- **What to provide:** Test plans, results of simulations, and details of any weaknesses identified and remediated.
- **Example:** A report from a red team exercise testing EDR capabilities.

Section 4: Logging and Monitoring

4.1 **Is a SIEM system deployed for centralized log management and analysis?**

- **What to provide:** Evidence of SIEM deployment, screenshots of SIEM dashboards, and sample use cases.
- **Example:** A screenshot from Splunk showing aggregated logs and configured alerts.

4.2 **Are logs configured to capture critical events (e.g., privilege escalation, lateral movement)?**

- **What to provide:** Log configuration files and examples of captured critical events.
- **Example:** A log entry showing a privilege escalation event.

4.3 **Are log retention policies aligned with regulatory requirements?**

- **What to provide:** Retention policies, configurations in the logging system, and regulatory mappings.
- **Example:** A policy stating logs are retained for 7 years for compliance with 12 CFR Part 748.

4.4 **Are logs reviewed regularly for anomalies, and findings reported?**

- **What to provide:** Review schedules, reports from log reviews, and corrective actions.
- **Example:** A report identifying anomalous activity with recommendations for improvement.

4.5 **Are alert thresholds validated and tested for effectiveness?**

- **What to provide:** Test plans, test results, and examples of threshold adjustments.
- **Example:** Documentation showing an adjustment to reduce false positives for failed login alerts.

Section 5: Incident Response and Recovery

5.1 **Is there a documented Incident Response Plan (IRP), and is it reviewed annually?**

- **What to provide:** The IRP document, records of annual reviews, and updates.
- **Example:** A review log showing updates to address ransomware-specific incidents.

5.2 **Are regular incident response drills conducted, including ransomware scenarios?**

- **What to provide:** Drill schedules, scenarios tested, and reports of results.
- **Example:** A report showing results from a ransomware drill and areas for improvement.

5.3 **Are roles and responsibilities within the IRP clearly defined?**

- **What to provide:** Role definitions, contact lists, and escalation procedures in the IRP.
- **Example:** A table of roles and responsibilities from the IRP.

5.4 **Are lessons learned from incidents incorporated into the IRP?**

- **What to provide:** Post-incident reports, meeting minutes discussing lessons learned, and updated IRP sections.
- **Example:** A revised IRP section addressing a previously overlooked ransomware vector.

5.5 **Are post-incident reviews documented and shared with stakeholders?**

- **What to provide:** Post-incident reports, meeting minutes, and action plans shared with stakeholders.
- **Example:** A post-incident review following a phishing attack, highlighting improvements to training.

Section 6: Network and Endpoint Security

6.1 **Is network segmentation implemented to isolate critical resources (e.g., databases, backups)?**

- **What to provide:** Network architecture diagrams, firewall rules, or VLAN configurations.
- **Example:** A network diagram showing segmented zones with restricted access to a database VLAN.

6.2 **Are inter-zone communications restricted using firewalls or NAC?**

- **What to provide:** Firewall rule sets, NAC configurations, and logs of access attempts between zones.
- **Example:** A firewall configuration allowing only specific services (e.g., database queries) between zones.

6.3 **Are unused ports, protocols, and services disabled on all systems?**

- **What to provide:** System configurations, vulnerability scan results, and hardening checklists.
- **Example:** A report from a vulnerability scanner showing closed unnecessary ports like Telnet (port 23).

6.4 **Are firewalls, IDS/IPS, and endpoint protections updated regularly?**

- **What to provide:** Update schedules, logs from update tools, and version details of security systems.
- **Example:** Logs showing the latest update for an IDS/IPS solution like Snort or Palo Alto.

6.5 **Are anomaly detection systems in place to monitor network traffic?**

- **What to provide:** Documentation of deployed anomaly detection tools, examples of alerts, and dashboards.
- **Example:** A screenshot of an anomaly detection system alerting on unusual traffic spikes.

Section 7: Privileged Access Management

7.1 **Is privileged access protected by MFA and restricted to authorized roles?**

- **What to provide:** Privileged access policies, MFA configuration for admin accounts, and role assignments.
- **Example:** An access control matrix showing roles and corresponding privileges.

7.2 **Are privileged account activities monitored and logged for review?**

- **What to provide:** Logs of privileged account activities and procedures for regular review.
- **Example:** A log entry showing an admin account's access to a critical system.

7.3 **Are Just-In-Time (JIT) access policies enforced for administrative tasks?**

- **What to provide:** JIT configurations, policy documents, and logs showing

temporary access assignments.
- **Example:** A log showing a JIT access request for a maintenance task, with automatic revocation.

7.4 **Are privileged accounts reviewed quarterly for appropriateness of access?**
- **What to provide:** Access review schedules, reports of findings, and evidence of corrections made.
- **Example:** A review report showing removed access for accounts no longer needing privileged access.

7.5 **Is there a process for revoking access immediately upon termination or role change?**
- **What to provide:** Termination checklists, process workflows, and logs of account deactivations.
- **Example:** A deactivation log showing immediate revocation of access upon employee termination.

Section 8: Security Awareness and Training

8.1 **Is annual security awareness training conducted for all employees?**
- **What to provide:** Training schedules, attendance records, and training content.
- **Example:** A list of training modules completed by employees in the past year.

8.2 **Are phishing simulations conducted to test employee readiness?**
- **What to provide:** Phishing test schedules, results, and improvement actions.
- **Example:** A report showing 90% success in identifying phishing attempts during the latest simulation.

8.3 **Are training materials updated to address new threats?**
- **What to provide:** Revision logs of training content and examples of updated material.
- **Example:** A new training module on the risks of AI-generated phishing emails.

8.4 **Are training results tracked to identify high-risk areas?**
- **What to provide:** Training dashboards and analytics showing performance metrics.
- **Example:** A report identifying employees with repeated failures in phishing tests.

8.5 **Is additional training provided for employees who fail phishing tests?**
- **What to provide:** Documentation of remedial training programs and completion records.
- **Example:** Attendance records of a special training session for high-risk employees.

Section 9: Change and Configuration Management

9.1 **Is there a documented change management policy, including CAB approval?**
- **What to provide:** The policy document, CAB meeting minutes, and approval logs.
- **Example:** A change request showing CAB approval before deployment.

9.2 **Are system configurations reviewed quarterly for deviations from baselines?**
- **What to provide:** Review schedules, deviation reports, and corrective actions.
- **Example:** A report identifying and correcting deviations in firewall configurations.

9.3 **Are all configuration changes tested, validated, and documented before deployment?**
- **What to provide:** Test plans, validation results, and change request

documentation.
- **Example:** A test log showing validation of a server patch before deployment.

9.4 **Are rollback procedures included in configuration management plans?**
- **What to provide:** Rollback plans, examples of tested rollbacks, and success reports.
- **Example:** A successful rollback of a failed software update.

9.5 **Are automated tools used to enforce configuration standards?**
- **What to provide:** Tool documentation, enforcement logs, and configuration baselines.
- **Example:** Logs from Ansible or SCCM showing compliance enforcement.

Section 10: Data Protection and DLP

10.1 **Is a DLP solution deployed to monitor and block unauthorized data transfers?**
- **What to provide:** DLP deployment documentation, examples of blocked attempts, and policies.
- **Example:** A log showing a blocked attempt to transfer sensitive data via email.

10.2 **Are sensitive data repositories restricted to authorized users?**
- **What to provide:** Access control lists, role assignments, and evidence of periodic access reviews.
- **Example:** A list of authorized users for a SharePoint folder with sensitive data.

10.3 **Are data transfer tools (e.g., rclone.exe) restricted or monitored?**
- **What to provide:** Logs of monitored tools, policies, and reports of blocked unauthorized tools.
- **Example:** A policy document prohibiting unapproved data transfer tools.

10.4 **Are DLP policies tested for effectiveness through simulated exfiltration attempts?**
- **What to provide:** Test plans, results of simulated attacks, and actions taken to improve policies.
- **Example:** A report showing a simulated data exfiltration attempt successfully blocked.

10.5 **Are employees trained on secure data handling policies?**
- **What to provide:** Training schedules, attendance records, and training materials.
- **Example:** A completed training module on secure data sharing practices.

Section 11: Testing and Continuous Improvement

11.1 **Are vulnerability scans conducted on all systems at least quarterly?**
- **What to provide:** Scan reports, schedules, and evidence of remediated vulnerabilities.
- **Example:** A Nessus scan report identifying and addressing critical vulnerabilities.

11.2 **Is penetration testing performed to identify and mitigate weaknesses?**
- **What to provide:** Penetration testing results, remediation reports, and test schedules.
- **Example:** A red team test report highlighting and addressing network vulnerabilities.

11.3 **Are corrective actions from tests tracked and verified for effectiveness?**
- **What to provide:** Tracking logs, reports, and follow-up test results.

- **Example:** A spreadsheet showing completed actions from a vulnerability assessment.

11.4 **Are testing results reported to senior management and the board?**
- **What to provide:** Meeting minutes, reports, and presentation slides.
- **Example:** A presentation to the board summarizing findings from the latest penetration test.

11.5 **Is the testing schedule updated to reflect emerging threats?**
- **What to provide:** Schedules, threat intelligence inputs, and updates to testing plans.
- **Example:** An updated plan including tests for AI-based malware.

Section 12: Compliance and Audit

12.1 **Are periodic audits conducted to evaluate security controls and compliance?**
- **What to provide:** Audit schedules, reports, and evidence of completed audits.
- **Example:** A compliance audit report for adherence to 12 CFR Part 748.

12.2 **Are audit findings documented, and remediation plans tracked?**
- **What to provide:** Audit logs, remediation plans, and completion evidence.
- **Example:** A tracker showing resolved audit findings.

12.3 **Are audit logs preserved for forensic analysis for at least 12 months?**
- **What to provide:** Retention policies and log preservation configurations.
- **Example:** SIEM configurations showing logs retained for 12 months.

12.4 **Are board-level reports prepared on security program status and incidents?**
- **What to provide:** Meeting minutes, board reports, and presentations.
- **Example:** A slide deck summarizing incident response activities for the board.

12.5 **Are independent reviews conducted to validate control effectiveness?**
- **What to provide:** Reports from third-party assessments or external auditors.
- **Example:** A third-party penetration test report.

Section 13: Vendor and Third-Party Management

13.1 **Are vendors required to comply with the institution's security policies?**
- **What to provide:** Vendor agreements, contracts with security clauses, and compliance documentation.
- **Example:** A contract clause requiring vendors to adhere to your organization's security standards, such as encrypting sensitive data and applying MFA.

13.2 **Are due diligence and risk assessments conducted for all third-party relationships?**
- **What to provide:** Vendor risk assessment reports, due diligence checklists, and risk categorization documentation.
- **Example:** A risk assessment report for a cloud service provider detailing their compliance with SOC 2 or ISO 27001 standards.

13.3 **Are third-party access and activities monitored for compliance?**
- **What to provide:** Logs of vendor access, monitoring reports, and documentation of corrective actions taken if non-compliance is detected.
- **Example:** Logs from a monitoring tool showing vendor access to the internal network, with regular compliance reviews.

13.4 **Are incident response capabilities of third parties reviewed periodically?**
- **What to provide:** Vendor incident response policies, periodic review schedules, and reports documenting the findings of these reviews.
- **Example:** A vendor-provided document detailing their process for handling and

reporting security incidents.

13.5 **Is vendor access promptly removed upon contract termination?**

- **What to provide:** Termination checklists, logs of access revocation, and evidence of offboarding processes.
- **Example:** A log showing that VPN credentials and system access for a terminated vendor were disabled within 24 hours of contract termination.

13.6 **Are third-party audits or certifications (e.g., SOC 2, ISO 27001) reviewed regularly?**

- **What to provide:** Copies of vendor audit reports or certifications and documentation of their annual review.
- **Example:** A SOC 2 Type II report reviewed and signed off by your risk management team.

13.7 **Are security responsibilities clearly defined in third-party contracts?**

- **What to provide:** Vendor contracts with sections outlining security responsibilities, SLAs, and penalties for breaches.
- **Example:** A contract specifying that the vendor must notify your organization within 24 hours of a security breach.

13.8 **Are vendor access rights regularly reviewed and updated?**

- **What to provide:** Access review schedules, logs of access rights modifications, and evidence of review results.
- **Example:** A quarterly review report showing adjustments to vendor access based on updated requirements.

13.9 **Are tools or processes used to track and monitor vendor activities (e.g., CASB, SIEM)?**

- **What to provide:** Screenshots of tools used for monitoring, reports on vendor activities, and examples of alerts triggered by vendor actions.
- **Example:** A CASB dashboard showing monitored file uploads by a vendor to cloud storage.

13.10 **Are third-party vendors included in business continuity and incident response plans?**

- **What to provide:** Copies of business continuity and incident response plans mentioning third-party integration, as well as testing results.
- **Example:** An IRP section outlining the role of cloud vendors in a disaster recovery scenario, with test results validating vendor response times.