corsica technologies

FINANCIAL SERVICES COMPLIANCE CHECKLIST

This checklist assumes FFIEC and FINRA compliance requirements.

Audits and Assessments

- [ ] Does your organization conduct a Business Impact Analysis (BIA)?
- [ ] Does your organization conduct an annual assessment of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data?
- [ ] Does your organization identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process?

Security Monitoring

- [ ] Does your organization have an SIEM solution in place?
- [ ] Is all security event information logged, continuously tracked, and reviewed?
- [ ] Does your organization utilize anti-malware technologies to detect and eradicate malicious code?
- [ ] Does your organization utilize File Integrity Monitor (FIM) technology to detect and report unauthorized changes to system files and configurations?
- [ ] Does your organization proactively govern account management of individual, group, system, application, guest and temporary accounts?
- [ ] Does your organization have solutions to prevent identity theft from occurring, and identify it, if it occurs?
- [ ] Does your organization document, monitor and report cybersecurity and privacy incidents?
- [ ] Does your organization incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents?
- [ ] Does your organization implement independent layers of security that minimizes interactions and dependencies by other layers?
- [ ] Does your organization define, control and review remote access methods?

FINANCIAL SERVICES COMPLIANCE CHECKLIST

corsica technologies

Vulnerability Management

- [ ] Does your organization facilitate the implementation and monitoring of vulnerability management controls?
- [ ] Does your organization address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks?
- [ ] Does your organization detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications?

Intrusion Detection

- [ ] Does your organization use an intrusion detection system (IDS) to detect and/or prevent intrusions into the network?

Security Awareness

- [ ] Does your organization implement a threat awareness program that includes the ability to receive and share information among other organizations?
- [ ] Does your organization facilitate the implementation of security awareness training?
- [ ] Does your organization provide role-based security-related training:
  - [ ] Before authorizing access to the system or performing assigned duties;
  - [ ] When required by system changes; and
  - [ ] Annually thereafter?
- [ ] Does your organization maintain situational awareness of evolving threats?
- [ ] Does your organization provides specific training for privileged users to ensure privileged users understand their unique roles and responsibilities?

Policies and Procedures

- [ ] Does your organization have policies and procedures that ensure media and data are retained in accordance with applicable statutory, regulatory and contractual obligations?
- [ ] Does your organization develop, govern & update procedures to facilitate the implementation of network security controls?

FINANCIAL SERVICES COMPLIANCE CHECKLIST

corsica technologies

Incident Response

- [ ] Does your organization facilitate the implementation of incident response controls?
- [ ] Does your organization's incident handling processes cover preparation, detection and analysis, containment, eradication and recovery?
- [ ] Does your organization regularly update incident response strategies to keep current with business needs, technology changes and regulatory requirements?
- [ ] Does your organization coordinate incident response testing with organizational elements responsible for related plans?
- [ ] Does your organization establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and privacy incident response operations?
- [ ] Does your organization perform digital forensics and maintain the integrity of the chain of custody?
- [ ] Does your organization utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement?

Confidently meet compliance requirements with a Compliance Gap Review.

Our team of compliance experts has deep expertise helping financial services organizations reach and maintain full compliance in accordance with strict industry regulations.

Every compliance gap review includes:

- A comprehensive analysis of your technology and cybersecurity environment.
- A review of your potential cybersecurity gaps and compliance risks.
- A plan customized for your organization with actionable steps to help mitigate risks and protect client data.

GET STARTED

corsicatech.com/finance-gap

sales@corsicatech.com | 855.411.3387 | corsicatech.com