ioSENTRIX
Your Trusted Partner In Cyber Security

SAMA Cyber Security Compliance

Service Overview

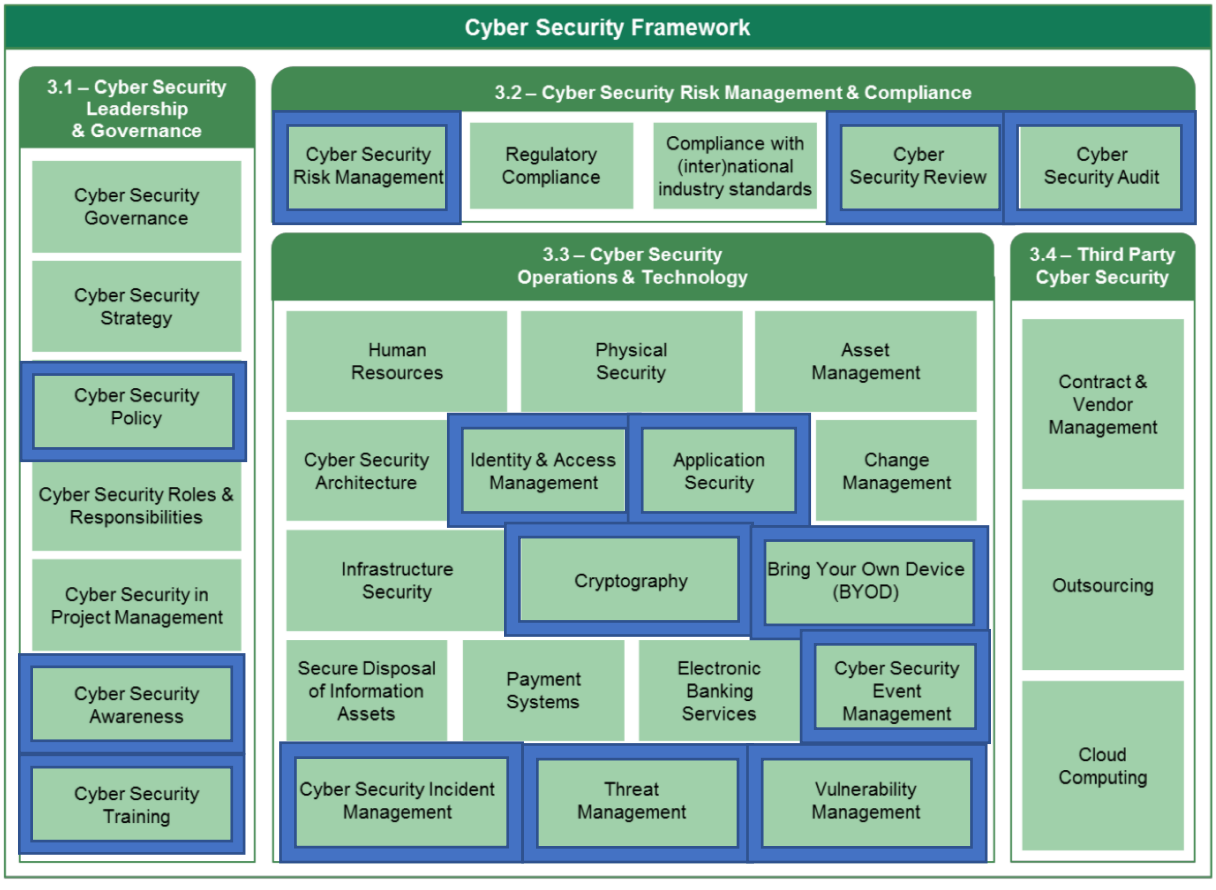
Background

To battle against the cyber threats, the Saudi Arabian Monetary Authority (SAMA) established a Cyber Security Framework version 1.0 in May 2017. The newer version 2.0 has been published in July 2018. This framework guides SAMA regulated entities referred to as "Member Organizations" to ensure that appropriate cybersecurity governance is established and followed. The Member organizations consist of local and foreign banks, insurance companies, money exchangers and other financial organizations.

SAMA Cyber Security Framework is based on NIST and ISO 27001 ISMS standard. ioSENTRIX has helped many clients to comply with such standards. We provide managed services in various domains such as Penetration Testing (for both Infrastructure and Applications), Vulnerability Management, SOC and SIEM management that can be leveraged meet the compliance requirements.

Our Approach

SAMA Cyber Security Framework contains the following Domain and Sub-domains. ioSENTRIX can provide managed services across the highlighted areas that can reduce the burden on the organization to meet the compliance requirements.



3.1 Cyber Security Leadership & Governance

- **Cyber Security Policy:** ioSENTRIX can develop Policies, Standards, Procedures, and Guidelines based on the business needs that comply with the industry's best practices.
- **Cyber Security Awareness:** We can develop programs and execute on the organization's behalf to raise cyber security awareness among the employees, customers and the third-party partners. We can conduct awareness campaigns, seminars and measure the effectiveness periodically for reporting.
- **Cyber Security Training:** We can develop and deliver custom security trainings based on the organization's security maturity level.

3.2 Cyber Security Risk Management & Compliance:

- **Cyber Security Risk Management:** ioSENTRIX can develop and implement a Risk Management framework and processes for the organization. We can define the process of risk identification (security into SDLC, Code Review, and Penetration Testing), risk analysis (assigning severity to different risks), and resolution (acceptance vs. mitigation).
- **Cyber Security Review:** We will conduct periodic penetration testing, vulnerability scanning of applications, infrastructure and other critical assets (whether internal or external) on the organization's behalf.
- **Cyber Security Audit:** We will assist in a third-party security Audit and help in remediating any outstanding risks that are found during the audit.

Our Capabilities

- Risk Management
- Cyber Security Policy, Procedure and Standard development
- Application Security
- Network and Infrastructure Security
- Penetration Testing
- Vulnerability Assessment
- Managed SOC and SIEM services

3.3 Cyber Security Operations and Technology:

- **Identity and Access Management (IAM):** We will help the organization to improve or implement IAM policies and the technologies according to industry's best practices and the SAMA compliance requirements.
- **Application Security, Infrastructure Security, and Event Management:** We will develop and implement Security into the SDLC model. We will define security requirements, application security certification program (prior to release) and pentest those applications. We will provide managed SIEM and SOC services so the organization can focus on their business without worrying about security.
- **Cryptography:** We can help develop a standard based on industry's best practices for Cryptography usage within an organization. This includes key generation, primitive usage, key management, revocation, and escrow.
- **Cyber Security Incident Management:** We provide incident management and response as a managed service that could be used by an organization to stay worry-free.
- **Threat & Vulnerability Management:** We can define the Threat and Vulnerability Management process for the organization in detail that could help them achieve SAMA compliance.

Why ioSENTRIX?

Lead by best expert in Cyber Security who has over 16 years of experience in helping various organizations. Our leader has worked with all major financial organizations in the US such as:

- Bank of America
- JP Morgan Chase
- Morgan Stanley
- Wells Fargo
- VISA
- American Express
- Mastercard

Why ioSENTRIX?

Lead by best expert in Cyber Security who has over 16 years of experience in helping various organizations. Our leader has worked with all major financial organizations in the US such as Bank of America, JP Morgan Chase, Morgan Stanley, Wells Fargo, VISA, American Express, Mastercard and other FinTech industries.

About ioSENTRIX:

ioSENTRIX LLC is a Security Consulting firm. We provide a wide range of security consulting services to our clients worldwide. Our list of clients spans the fortune 500, large enterprises to small start-ups, financial institutions, and several high-tech companies.

We are an innovative consulting company offering a full range of cyber security services to businesses of all sizes, tailored to meet any budget requirements. We help our clients by identifying, mitigating and preventing vulnerabilities in their software, infrastructure, and cloud.

We offer a comprehensive vulnerability assessment that includes design-review, threat model, penetration test, code review, and open source software security. We've got the necessary tools and the expertise to secure your business so you can focus on growing it.

Learn more about our services at **https://www.iosentrix.com.**

ioSENTRIX LLC.

150 S. Sterling Blvd, Suite 543
Sterling Virginia 20164 (USA)

Sales: 1 (888) 958-0554
Email: sales@iosentrix.com