Executive Summary

Information security is an essential component of governance and management that affects all aspects of entity-level controls. Coforge Security assessment program includes appropriate information security evaluations throughout its assessment universe. Coforge ensures that the process of assessing the design and operating effectiveness of information security management does receive the focus it requires.

Coforge Cybersecurity Service Line provides advisory on governance, policy, enforcement, monitoring and innovation necessary for the modern business to establish cost-effective information security processes, while providing adequate information security assurance within the risk appetite and budget of the organization.
Need for Information Security Assessment

The risks associated with inadequate information security management include:

- Information security strategies not aligned with IT or business requirements
- Information security value (cost-benefit) structure not aligned with business needs or goals
- Undefined or confusing information security accountability
- Noncompliance with internal and external requirements
- Ineffective use of financial resources allocated to information security
- Information security not included in portfolio selection and maintenance and/or architecture design resulting in ineffective, inefficient or misguided information security solutions
- Information security not monitored and policies not applied uniformly with varying enforcement

Information security is about minimizing exposures, based upon risk management. Failure to implement and monitor risk mitigation processes in one area may compromise the entire organization.

Coforge Information Security Assessment Service

Coforge Information Security Assessment or Risk Assessment services include the process of identifying, estimating and prioritizing information security risks.

Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact on the organization and the likelihood that such circumstances or events will occur.

Coforge Approach for Information Security Assessment

Meet Compliance Requirement: An effective cyber risk assessment helps organizations prioritize risks, map risks to the applicable risk owners, and effectively allocate resources to risk mitigation.

Perform Gap Analysis/Cyber Exposure: Gap analysis is intended to highlight the amount by which the need exceeds the resources that exist and what gaps may need to be filled to be successful.

Identify Vulnerabilities: Cyber risk assessment helps determine security flaws and overall risk to have a better understanding of the assets and to reduce the likelihood of a breach.

Discover Assets: Proactively discover true asset identities (rather than IP addresses) across any digital computing environment and keep a live view of your assets with a cyber-risk assessment.

Baseline: Understanding security controls. It helps create a standard which company uses in future to assess organizations.
Coforge Information security assessment Services under its GRC Service Offering covers the following areas of Assessment:

- Management direction, including policy creation, involvement in significant information security strategies, establishment of and adherence to an information security architecture, and alignment of information security strategies with business strategies

- Management oversight and execution of essential information security operations. The former focuses on routine operations that affect information security, including access control; user identity management; and configuration management of other security building blocks, including intrusion detection and penetration testing systems, antimalware, and other processes. The latter includes information security incident management and security forensics.

- Management of information security technologies utilized within the organization.

**Objectives of Information Security Management Assessment Review**

The information security management assessment review will:

- Provide Client management with an assessment of the effectiveness of the information security management function

- Evaluate the scope of the information security management organization and determine whether essential security functions are being addressed effectively

**Note:** It is not designed to replace or focus on audits that provide assurance of specific configurations or operational processes.

**Scope of Review**

The review will focus on:

- Information Security Management Processes associated with governance, policy, monitoring, incident management and management of the information security function

- Information Security Operations Management Processes associated with the implementation of security configurations

- Information Security Technology Management Processes associated with the selection and maintenance of security technologies

**ISACA IT Assurance Framework and Standards**

ITAF section 3630.7 Information Security Management is of primary relevance to the assessment of information security management. However, information security management is pervasive throughout the IT organization and its functional responsibility. Components of information security are also included in the following ITAF sections:

- 3410 IT Governance
- 3425 IT Information Strategy
- 3427 IT Information Management
- 3450 IT Processes
- 3630 Auditing IT General Controls
ISACA Control Framework

COBIT is a framework for the governance of IT and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework from which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

COBIT IT process DS5 Ensure systems security, from the Deliver and Support (DS) domain, is the primary control framework and addresses good practices from ISO 27001, NIST, PMI, ITIL and other frameworks for ensuring security of corporate information.

Assessment Skills

Information security management addresses many IT processes. Since the focus is on the management of information security, the assessment professional from Coforge will have the requisite knowledge of the scope and requirements of information security, governance of IT and the information security components therein, information security components of IT architecture, risk management, and the direct information security processes.

In addition, this assessment program addresses organizational human resource reporting, management planning and senior management interfaces. Therefore, the assessment professional conducting the assessment will have the requisite experience and organizational relationships to effectively execute the assurance processes.

The following are the areas that shall be scoped as part of the assessment program by Coforge basis the necessity and the risk profile of the client:

- **Management of IT security** - Manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements.

- **IT security plan** - Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

  - **Identity management** - The information security function has defined policies and monitors activities relating to unique user identification; authentication mechanisms; user access rights according to job definition; and documented, appropriate authorization and approval mechanisms.

  - **User account management** - The information security function has established policies and monitoring procedures that address: requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. The process includes an approval procedure outlining the data or system owner granting the access privileges and applies to all users, including administrators (privileged users) and internal and external users, for normal and emergency cases.

  - **Security testing, surveillance, and monitoring** - Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.
• **Security incident definition** - The security incident management process is defined and monitored by the information security function, and an incident response team has been established and is operationally effective.

• **Protection of security technology** - Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

• **Cryptographic key management** - Policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.

• **Malicious software prevention, detection, and correction** - Preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

• **Network security** - Information security management is included in the selection, implementation and approval of security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.

• **Exchange of sensitive data** - Information security has approved policies concerning the exchange of sensitive transaction data through a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and nonrepudiation of origin. All incidents involving the exchange of sensitive data are reported through the incident reporting system and are directed to the CIRT team.

---

**Our Success Stories**

• Leading railway company in Europe, vast international rail network encompassing 9 countries in Europe. Challenges were to perform security assessment, and redefining governance, risk, and compliance processes. Solution provided by doing GAP assessment of procedures. Benefits to client ranged from compliance of monthly patching, risk score improvement.

• A leading US print media company, provides the customer with an assessment of IT policies, procedures, technologies, and operating effectiveness. Identifying factors affecting reliability, accuracy, and security of the enterprise data due to weaknesses in security control. Propose and evaluate the effectiveness of response and recovery programs.

• One of US top Heal and Medicare solutions provider, Provided the customer a tiered evaluation and deliver report with findings and recommendation to mitigate threat and vulnerabilities as a roadmap to comply and agree up on maturity levels of Cyber security.

• One of world’s largest trading company with Japanese base, Challenges included to perform the FFIC assessment prior to audits and defining security processes for risk management and compliance management. Solution provided conducting workshops and stakeholders to understand the environment. Conducted FFIC assessment of the customer’s environment. Evaluations to perform identification gaps and improvement areas.
Coforge is a global digital services and solutions provider, that leverages emerging technologies and deep domain expertise to deliver real-world business impact for its clients. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge’s proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.

Learn more about Coforge at: www.coforge.com

Stay connected:  

---

For more information, contact information@coforge.com

© 2022 Coforge. All rights reserved.