# Policy – Information Security Risk Management

## 1. Objective:

The Policy is intended to ensure that GlobalLogic takes appropriate steps to identify, prioritize, monitor and minimize or eliminate any potential information security risks to the information assets operated within the scope of the Information Security Management System (ISMS).

## 2. Scope

GlobalLogic employees/consultants who participate in information security risk management activities within the scope of the ISMS.

# Abbreviations and Definitions

| Abbreviation | Description |
|---|---|
| **Asset** | Anything that has value to the organization and is directly involved in business processes performing. |
| **Asset Owner** | An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. |
| **Control** | An organizational, procedural, or technological means of managing risk; a synonym for safeguard or countermeasure. |
| **Impact** | The overall business loss expected when a threat exploits vulnerability against an asset or overall business improvement expected when opportunities are executed |
| **ISMS** | Information Security Management System. |
| **Residual risk** | Risk remaining after risk treatment. |
| **Risk management** | The continual process of identifying vulnerabilities and threats to the information assets, considering the impact and the likelihood of harmful events occurring, and determining the measures to provide appropriate level of protection against the identified threats. |
| **Risk treatment** | The process of selecting and implementing measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. |

| | |
|---|---|
| **Risk owner** | An individual or entity that is responsible for treatment of particular risk. Usually Head of Function responsible for appropriate security systems and controls. Maybe an Asset Owner. |

## 3. Description

Risks to information assets within the scope of ISMS are identified, evaluated, prioritized, assessed, treated, monitored and reviewed regularly.

Information security risk assessments are performed on an annual basis or when significant changes are proposed or occured. Risk assessments may also be initiated based on audit or control assessment results.

Risk assessment and treatment procedures are defined in the Procedure – Risk Management which contains necessary instructions of how these activities have to be performed.

Risk management activities are performed in GlobalLogic to identify risks that may affect Company's business interests, operations, reputation and cause financial losses or violation of legal or regulatory requirements and plan appropriate actions to avoid unacceptable losses. Risk assessment is mandatory for critical information assets and optional for non-critical assets.

The execution, development and implementation of remediation programs are the joint responsibility of the Information Security Officer and the respective Function Head/Project Manager responsible for the system area being assessed. Employees/consultants are expected to fully cooperate with any risk assessment being conducted on systems for which they are held accountable. Employees/consultants are further expected to collaborate with the Information Security Officer in the development and implementation of a remediation plan as set in **Procedure - Risk Management**.

## 4. Policy Compliance

The Information Security Officer will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the Head of Security Risk & Compliance in advance.

# Change History

| Revision | Change Description | Valid Date | Approver |
|---|---|---|---|
| 1.0 | Initial issue (ISMS documentation structure review) | 01/27/2021 | Alok Malik, CISO |
| 2.0 | Policy – Information Security Risk Management, operated in India, was merged with global Policy – Risk Assessment as part of the documentation unification process. Name of the Policy was changed to Policy – Information Security Risk management after documents merge. | 09/22/2021 | Alok Malik, CISO |
| 2.0 | Annual review – no changes | 09/09/2022 | Alok Malik, CISO |
| 2.0 | Annual review – no changes | 09/21/2023 | Denys Kudriavchenko, Head of Security Risk & Compliance |