
IT Governance, IS Policy, Role of CISO, IT Management

(Module -1 : DISSA Course)

Arijit Chakraborty

26.12.2021

GOVERNANCE, SECURITY POLICIES AND CONTROLS-

Role of IS Audit

- IS audit being a process of **collecting and evaluating evidence/information** to determine whether a computer system could:
 - (a) **Safeguard its assets** (hardware, software and data) through adoption of adequate security control measures;
 - (b) **Maintain data integrity;**
 - (c) **Achieve goals** of the organization effectively; and
 - (d) **Result in the efficient use** of the available Information System resources.

Governance and Management of IT

- Proper IT governance cannot be achieved without a top-down approach.
- Top management needs to be driving the governance.
- Done through a steering committee comprised of top executives who set the strategic direction & policies that align with the business' goals
- Organizations, broadly have 2 committees
 - **IT Strategy committee & IT Steering committee**
- These policies, & associated risk appetite, are carried out through Chief Information Security Officers (CISO) or CIRO
- The CISO and CIRO are responsible for :
 - ✓ developing security policies,
 - ✓ handling incident management, (SIEM)
 - ✓ vulnerability management,
 - ✓ identity and access management.

The 5 domains of IT governance

- **ITGI** : IT Governance Institute (a division of ISACA) breaks down IT governance into 5 domains:
 1. Value delivery
 2. Strategic alignment
 3. Performance management
 4. Resource management
 5. Risk management

IT governance frameworks and models

1. King reports of corporate governance (versions I to IV).
2. ISO/IEC 31000:2018 (risk management).
3. ISO/IEC 27001:2013 (information security).
4. Business continuity management and disaster recovery.

Governance of Enterprise IT (GEIT):

- GEIT = domains of Corporate governance
- GEIT = system in which all stakeholders, including BoD, senior management, and departments provide input into the decision-making process.
- GEIT = responsibility of BoD and executive management.
- **Purposes of GEIT are:**
 - to direct IT endeavors to ensure that IT performance meets the objectives of aligning IT with the enterprise's objectives and the realization of promised benefits
 - enable the enterprise by exploiting opportunities and maximizing benefits
 - IT resources should be used responsibly, and IT-related risk should be managed Appropriately
- Key element of GEIT = alignment of business and IT, leading to the achievement of business value.

ISO 38500 –international IT Governance Standard

- Sets out principles, definitions and a high-level framework that organisations of all types and sizes can use to better align their use of IT with organisational decisions, and meet their legal, regulatory and ethical obligations.
- ISO/IEC 38500:2015 is applicable **to all organizations**, including public and private companies, government entities, and not-for-profit organizations. ISO/IEC 38500:2015 is applicable to organizations **of all sizes** from the smallest to the largest, regardless of the extent of their use of IT.

ISO 38500

- ISO/IEC 38500 = guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of IT within their organizations.
- *seeks to establish that IT is the entire executive management team's responsibility, and not just dependant on the CISO*
- *Addresses = responsibility of appraising IT proposals, scrutinizing current projects and providing guidelines for improved IT policies*
- *ISO 38500's objective = to provide a framework of principles that directors can use when evaluating, directing and monitoring the use of IT in their organizations*
- *ISO 38500 places strong emphasis on corporate governance*
- *ISO 38500 standard expects directors to provide a set of IT principles and oversee the implementation (which includes approvals)*

A. Role of IT strategy committee:

- Advises the board and management on IT strategy
- Is delegated by the board to provide input to the strategy and prepare its approval
- Focuses on current and future strategic IT issues
- Provides insight and advice to the board on topics such as:
 - ❑ The alignment of IT with the business direction
 - ❑ The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
 - ❑ The achievement of strategic IT objectives

- **Membership of IT Strategy committee:**
 - Board members, and
 - Specialist non-board members
 - **B. Role of IT Steering committee:**
1. Assists the executive in the delivery of the IT strategy
 2. Oversees day-to-day management of IT service delivery & IT projects
 3. Focuses on implementation
 4. Decides overall level of IT spending and how costs will be allocated
 5. Approves project plans and budgets, setting priorities and milestones
 6. Communicates strategic goals to project teams
 7. Monitors resource and priority conflict between enterprise divisions and the IT function as well as between projects
 8. Report to the board of directors on IS activities.
 9. Make decisions regarding centralization versus decentralization and assignment of responsibility.

- The **COBIT Process Assessment Model (PAM)**, using COBIT 5,
- **Capability Maturity Model Integration (CMMI)** – is a process improvement approach that provides enterprises with the essential elements of effective processes. It is based on ISO/IEC 15504 Information Technology—Process Assessment standard.
- CMMI have 5 maturity levels
 - **Level 1 – Initial** – This is a riskiest stage an organization can find itself – an unpredictable environment that increases risk and inefficiency.
 - **Level 2 – Managed** – Projects are planned and performed, however there are lot of issues to be addressed
 - **Level 3 – Defined** – Organizations are proactive at this level, rather than reactive. Processes are tailored for the organization. Organization is aware of their shortcomings, how to address and plans for improvement.
 - **Level 4 – Quantitatively managed** – This level is more measured and controlled. The organization is ahead of risks, with more data-driven insight into process deficiencies.
 - **Level 5 – Optimised** – At this stage, the processes are stable and flexible. The organization will be in constant state of improving and responding to changes or other opportunities.

Risk Management:

- The process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and what countermeasures to take in reducing risk to an acceptable level.
- encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes
- The Board may choose to treat the risk in any of the following ways

1. **Avoid**—Eliminate the risk by eliminating the cause
2. **Mitigate**—Lessen the probability or impact of the risk by defining, implementing and monitoring appropriate controls
3. **Share/Transfer** (deflect, or allocate)—Share risk with partners or transfer via insurance coverage, contractual agreement or other means
4. **Accept**—Formally acknowledge the existence of the risk and monitor it.

- ***Points to remember:*** *The best to assess IT risks is achieved by – evaluating threats associated with existing IT assets and IT projects.*
- **The 5 steps of Risk Management process involve:**
 - **Step – 1: Asset identification** – Examples: Information, Data, Software, Hardware, documents, personnel.
 - **Step – 2: Evaluation of threats and vulnerabilities:**

- ***Threat*** – A threat is a person or event that has the potential for impacting a valuable resource in a negative manner.
- ***Vulnerability*** – Vulnerability refer to weaknesses in a system. They make threat outcomes possible and potentially even more dangerous.

- **Step 3 : Evaluation of the impact** – The result of a threat agent exploiting a vulnerability is called an impact
 - In commercial organizations, threats usually result in
- a direct financial loss in the short term or
- an ultimate (indirect) financial loss in the long term

- **Step 4 – Calculation of Risk** – A common method of combining the elements is to calculate for each threat: **probability of occurrence × magnitude of impact**. This will give a measure of overall risk.
- **Step 5 – Evaluation of and response to Risk**
 - After risk has been identified, existing controls can be evaluated or new controls designed to reduce the vulnerabilities to an acceptable level.
 - These controls are referred to as countermeasures or safeguards and include actions, devices, procedures or techniques
 - Residual risk, the remaining level of risk after controls have been applied, can be used by management to further reduce risk by identifying those areas in which more control is required.

IS Security Control objectives

1. Information is **available and usable when required**, and the systems that provide it can **appropriately resist attacks and recover from failures** (*availability*)
2. Information is **observed by or disclosed to only those who have a right to know** (*confidentiality*)
3. Information is **protected against unauthorized modification** (*integrity*)
4. Business transactions as well as **information exchanges** between organization locations or with partners/ users **can be trusted** (*authenticity and non-repudiation*)

1.1.3. Controls

- (a) **Deterrent Controls:** Deterrent Controls are designed to deter unauthorised people, internal as well as external, from accessing the information and information systems.
 - (b) **Preventive Controls:** Preventive Controls prevent the cause of exposure from occurring or at least minimize the probability of the occurrence of unlawful events.
 - (c) **Detective Controls:** When a cause of exposure has occurred, detective controls report its existence in an effort to arrest further damage or minimize the extent of damage. Detective controls limit the losses, if an unlawful event at all occurs.
 - (d) **Corrective Controls:** Corrective Controls are designed to help the organization recover from a loss situation. BCP = corrective control. Without corrective controls in place, the organisation will suffer from the risk of loss of business and other losses, due to its inability to recover essential IT based services, information after disaster has taken place.
- IS Auditors will require to ascertain that **adequate control exists to cover each likely unlawful event**.
 - TOC : If the unlawful event is covered by a control, the IS auditors will require to evaluate whether the **control is operating effectively**. If more than one control covers an unlawful event (i.e., redundant controls), the IS auditors will require to verify that all these **controls operate effectively**.

Case 1 : Tata Steel : IS Policy

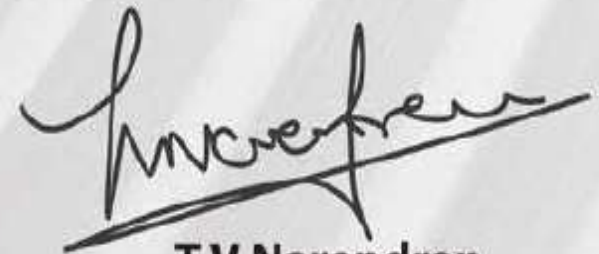
TATA STEEL



Information Security Risk Management Policy

- This policy shall provide a risk assessment framework as suited to, and as relevant to the business requirement of TSL.
- The information security risks for the identified Information Assets of TSL, covering business operations, vendors, and regulatory and or legal requirements shall be considered for management and mitigation.
- A formal mechanism of conducting Risk Assessments (RA) and execution of the Risk Treatment (RTP) plan shall be developed on all the identified assets of TSL on and off premises and those with the vendors.
- Risk assessment shall consider:
 - The business impact due to the occurrence of the threat,
 - The probability of the occurrence of that threat.
 - Risk Impact Rating which is the product of (Value of Threat x Probability or Likelihood of Occurrence) x Asset Value, will be the criterion used to identify the acceptable level of risk which will be developed and implemented.
 - A Threshold Value based on the outcome of step shall be decided for the purpose of the level above which a mitigating control will be deployed.

- Risk Treatment Plan shall consider all the aspects of Risk Treatment such as (Mitigation, Acceptance, Transfer and Avoidance).
- The execution, development and implementation of a Risk Assessment and Risk Treatment Plans shall be responsibility of the Information Security Organization as defined in the Information Security Organization Policy.
- TSL shall develop and or deploy adequate and sufficient controls to ensure that information security risks are reduced to an acceptable level commensurate with the risk appetite of the organization and any residual risk(s) thereof shall be acceptable to TSL after the application of supplementary controls.
- The Risk Assessment and Risk Treatment shall be reviewed periodically, should there be major changes to the business, organizational structure and regulatory landscape which will impact the information security posture of TSL.
- The effectiveness of the Risk Assessment and Risk Treatment approach shall be measured through the development of appropriate metrics, which will be reviewed periodically to ensure their relevance and adequacy.
- Any exception to this policy shall be managed by a formal process.



T V Narendran
CEO & Managing Director

Date : November 1, 2017

Information Security Asset Classification Policy

- Any asset which has a business value is to be considered as an information asset. This will include, but not be restricted to; information in digital and non digital format, portable media, network infrastructure devices (servers, routers, switches, modems, tape drives, storage devices, load balancers, ids, ips, firewalls), applications, services, desktops , laptops and mobile computing and communication devices, utilities such as power generation, conditioning and distribution equipment and air-conditioning equipment amongst others.
- Valuation of information assets shall take into account the Business Impact Parameters such as (Financial, Operational, Regulatory/Compliance, Competitive and Legal); should they be compromised in any manner.
- A score shall be assigned for each of the Business Impact Parameters against Business Impact Criteria such as HIGH, MEDIUM and LOW comprising point scale of 5, 2 and 0.5 respectively, to arrive at the Risk Impact Class.

- Risk Impact Class shall be categorised as CRITICAL, SIGNIFICANT, MODERATE AND NEGLIGIBLE. The Risk Impact Class (RIC) will lead to the classification of the Information Asset.
- All Information generated or in existence shall be clearly identified and an Information Asset Classification (IAC) template shall be drawn up by respective Department Implementer (DI). The IAC shall only be effective after approval from the authorized signatories.
- Labelling methods in pursuant to the classification modality shall be adopted.
- Retention Limits shall be defined for every category of the identified information asset in consonance with the requisite business, regulatory and legal requirements.
- The term 'owner' for an information asset is an individual or department which has a management approval and hence responsibility for controlling the production, development, maintenance, use and security of an asset. Owners shall set the security requirements for information assets and shall be responsible for communicating those requirements to all the custodians.
- Custodians shall be those who are the authorized employees/departments who shall have the custody of the Information Asset.
- There shall be a formal review mechanism to ensure that the listing of all Information Assets along with their valuation and classification is current, accurate and relevant.
- In order to measure the effectiveness of the process of the maintenance of the inventory of the Information Assets, stakeholders shall be evaluated against the metrics which have been defined. Corresponding actions and records shall form as supporting elements of the compliance process.
- Any exception shall be managed through a formal process.

A handwritten signature in black ink, appearing to read 'Anurag', is written over a horizontal line.