IS Policy, Role of CISO, IT Management

(Module -1 : DISSA Course)

Arijit Chakraborty

02.01.2022

Strategic plan for IT Department

(a) IT departmental **resource allocation ,** strategic utilization of IT = to optimize internal operations & profits

(b) The **skillsets required** in IT department, Managerial & personnel roles, along with departmental teams (e.g., VP of IT, CIO, CTO, R&D, IT security)

(c) Required IT systems of IT infrastructure

(d) The critical problems that IT department is envisioned to solve – currently and as the company grows

(e) Expectations of the stakeholders/investors, along with the agreed-upon long-term goals

(f) IT Department Structure (Adaptive and Evolve)

Module 1.1.1. - Information System (IS) Governance

(a) **Inappropriate Strategy for Information System:** Aligning informative strategy with business strategy = complicated & critical. Lack of alignment can lead to **mismanagement, inappropriate investments / ineffective implementation** of new system.

(b) **Laboriousness in Quantifying the Value of Informative System:** = necessary during disposals and acquisitions. The value derived from the impact of IT = Quantified. Absence of particular information = lead to improper investment decisions.

(c) **Reviewing Existing IS Security Controls: Test** by best parameters of the industrial standards. Making recommendations to strengthen IS controls.

(d) **Systems and Applications:** An audit to certify that systems and applications are appropriate to entity's requirements, are efficient, adequately controlled to ensure valid, reliable, well timed, and secured input, processing and output.

(e) **Business Application Audits:** Checking upon limitations, features and application capabilities for establishing the lawfulness in the applicant's logical access controls.

(f) Reviewing the **operational adequacy of application package**,

Auditing **SDLC process** and testing performance through different tools.

Centralized vs Decentralized IT Structures

- **Centralized Structure**: = where all **core IT systems and networks are managed by a central organization,** such that all systems can be easily integrated and managed from a single IT central hub.

(a) **Centralized Structure Pros**: Better Budget control, easier governance, better standardization, better alignment across the entire technology portfolio, easier project/workflow integration, more feasible IT management

(b) **Centralized Structure Cons**: may become bureaucratic, business departments may be unhappy

- fighting with other departments to get their tech initiatives prioritized.

- **Decentralized Structure**: = where management of critical IT components, system controls and networks is **distributed amongst multiple, different core IT centers** within the overarching enterprise IT infrastructure, allowing different sub-departments and teams to utilize different resources within their own sub-systems/intranets.

(a) **Decentralized Structure Pros**: Individual departments/business units have **more direct control over their tech projects** and priorities; generally decentralized groups can get faster results (less overhead & prioritization fights).

(b) **Decentralized Structure Cons**: Solutions optimized at department level **often result in inefficiencies at the enterprise level** ("silos" of disconnected data and business processes);

(c) too much departmental independence can **lead to integration challenges** and unnecessarily duplicative systems and data.

Sourcing Practices:

- Delivery of IT functions can include:
  - **Insourced –** Fully performed by the organization’s staff
  - **Outsourced** – Fully performed by the vendor’s staff
  - **Hybrid** – Performed by a mix of the organization’s and vendor’s staffs; can include joint ventures/supplemental staff
- IT functions can be performed across globe, taking advantage of time zones & arbitraging labor rates, can include:
  - **Onsite** – Staff work onsite in the IT department.
  - **Offsite** – staff work at a remote location in the **same geographic zone**
  - **Offshore**—Staff work at a remote location in a **different geographic region**

IT Delivery Models

- Developing in house IT capabilities to complete projects or provide services **can be costly & risky venture**, particularly when the IT needs of an organization are constantly changing.
- When companies look for outside help in fulfilling IT business needs, they generally consider 2 delivery models:

1. Staff Augmentation - allows organizations to add staff to their existing teams based on the additional skills required to support their initiatives. This model allows rapid access to missing capabilities and skills.

Or

2. Managed Services- allows it to free up specialist knowledge within organization and to focus on core business activities.

ITIL Framework

- ITIL framework offers **5 core processes** = align all business goals with IT infrastructure:

1. ***Service Strategy***: Aligning critical business goals/model with components and services of enterprise's IT infrastructure
2. ***Service Design***: The IT services that IT systems offer in order to support the business's operations
3. ***Service Transition***: The transition from a planning/developmental phase to an operational/management phase
4. ***Service Operation***: Operating all services according to SLA in place
5. ***Continual Service Improvement***: Analyzing and offering improvements for each service in order to increase service quality

Corporate Information Security (IS) Policy

(i) **Identify a member of senior management, as Chief Information Security Officer (CISO),** -designate as a 'Point of Contact', responsible for Co-ordinating security policy compliance efforts and to regularly interact with **Indian Computer Emergency Response Team (CERT**) in Department of Information Technology (DIT), nodal agency for cybersecurity.

(ii) **Prepare information security plan** and implement the security control measures as per IS/ISO/IEC 27001 & other guidelines/standards, as appropriate.

(iii) **Carry out periodic IT security risk assessments** & determine acceptable level of risks, consistent with criticality of business/functional requirements,

(iv) **assess likely impact on business/functions** and achievement of organizational goals/objectives.

v. Periodically test & evaluate adequacy & effectiveness of technical security control measures implemented for IT systems & networks.

vi. Test and Evaluation may become necessary after each significant change to the IT applications/systems/networks

- Penetration Testing (both announced & unannounced)
- Vulnerability Assessment
- Application Security Testing,
- Web Security Testing

vii. Carry out Audit of IS infrastructure on an annual basis & when **there is major upgradation/change** in IT Infrastructure, by an independent IT Security Auditing Firm

Role of CISO

- **ISO 27001** does not require a company to nominate a **Chief Information Security Officer (CISO)** , or any other person who would coordinate information security (e.g., Information security officer, Security manager, etc.).
- ISO 27001 is applicable to companies of any size, in any industry, so requiring small companies to have a designated CISO would be overkill.
- Hence **no generalisation of need for CISO**
- **Role of CISO**
- **What does the CISO do?**
- CISO should coordinate all the activities related to securing the information in a company,
- **1. Compliance:**
- Develop the list of interested parties related to information
- Develop the list of requirements from interested parties
- Remain in continuous contact with authorities and special interest groups
- Coordinate all efforts related to personal data protection

- **2. Documentation:**
- Propose the draft of main information security documents – e.g., **Information security policy**, Classification policy, Access control policy, Acceptable use of assets, **Risk assessment and risk treatment methodology**, **Statement of Applicability**, Risk treatment plan, etc.
- Be responsible for reviewing and updating main documents
- **3. Risk management:**
- Teach employees how to perform risk assessment
- Coordinate the whole process of risk assessment
- Propose selection of safeguards
- Propose the deadlines for safeguards implementation

- **4. Human resources management:**
- Perform background verification checks of job candidates
- Prepare the training and awareness plan for information security
- Perform continuous activities related to awareness raising
- Performing induction training on security topics for new employees
- Propose disciplinary action against employees performing security breach
- **5. Relationship with top management:**
- Communicate the benefits of information security
- Propose information security objectives, Report on the results of measuring
- Propose security improvements and corrective actions
- Propose budget and other required resources for protecting the information
- Notify top management about the main IS risks
- Report about the implementation of safeguards
- Advise top executives on all security matters

Post-COVID role of CISO

1. to quickly act on re-architecting security as per current business requirements and to update (and consolidate if needed) the assets & vendors that are working across the organizations
2. to have an updated view on the risk posture because of changes in the IT, adoption of new thinking
3. To meet expectation of the board and senior leadership on Cybersecurity and data privacy
4. to develop a more strategic toolkit for ensuring that the key message on cybersecurity is delivered to the board in terms of risk impact on the strategy and business implications of cyber-attack.
5. To procure separate Cybersecurity budget (from the IT budget
6. To ensure robust network security, MFA and privilege access management, 3rd party security, and ensuring secure remote access is scalable for employees that used to access the system only through desktop set-up.

CISO – Value Add

- **Value delivery**
- 1. Establish visibility of cyber security at senior management & board level
- 2. Quantify security maturity through scorecards
- 3. Put in to practice demonstrable savings criteria for security investments
- 4. improve overall situational awareness for entire company