NATIONAL BANK OF CAMBODIA

Riel. Stability. Development.

Technology Risk Management Guidelines Workshop

National Bank of Cambodia

21 August 2019

This presentation has been prepared for the purpose of workshop and BFIs should go through the regulation for better understanding of the requirements. View of the presenter may not necessarily be the view of NBC

Agenda

- Emerging Technology Risk
- Timelines for implementation
- Risk Management Guidelines Requirements
- Q&A Session

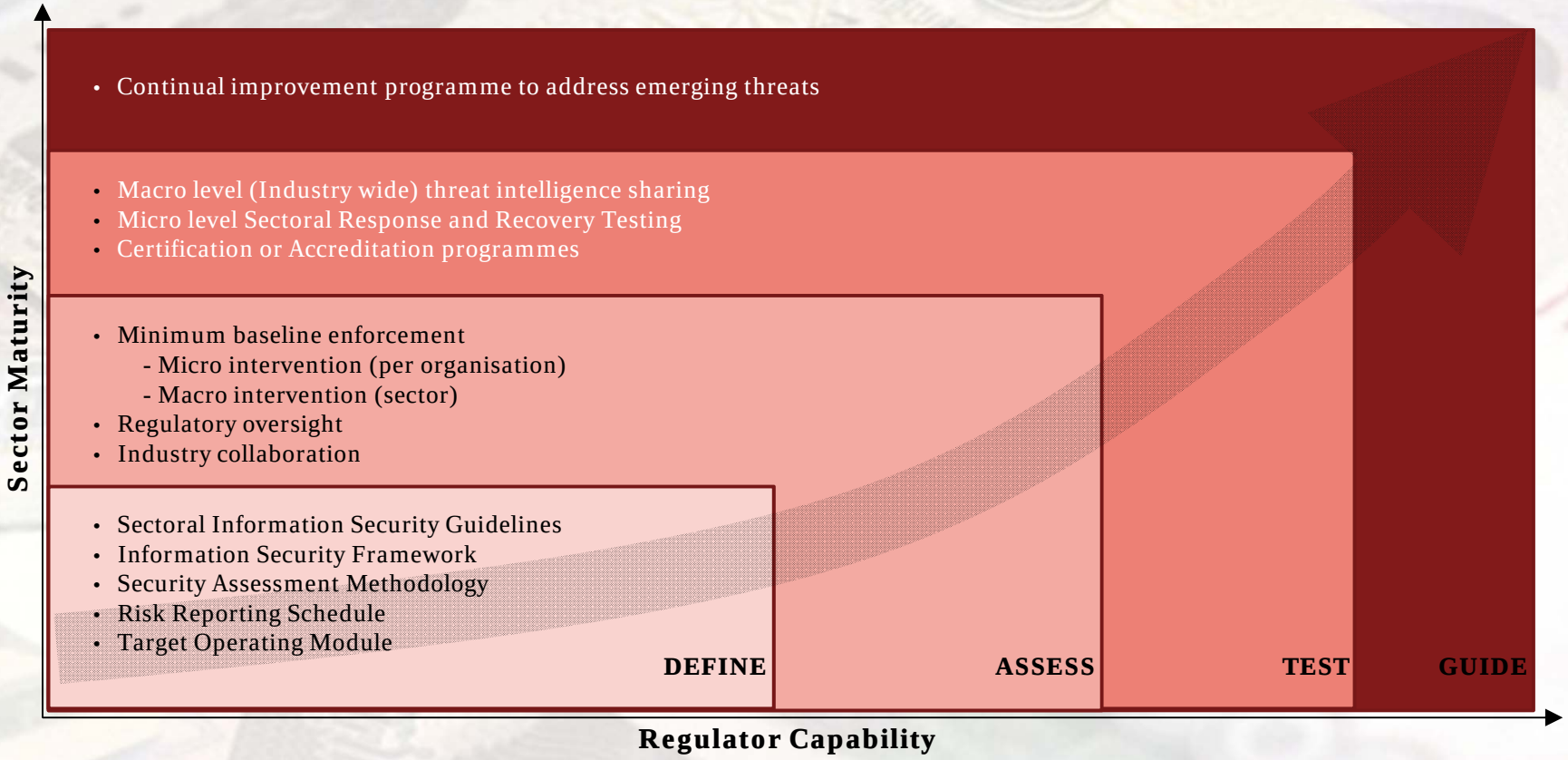
Changing Threat Landscape – Driver for Regulatory Intervention

	Generic Threats		*Financial Services Threats*				
Key Cyber Threat Scenario	Ransomware encrypting data and disrupting business operations	Reliance on internet service providers which are disrupted	Disruption of online services to create market volatility and damage reputation	Theft of funds from individuals and institutions by hacking payment services	Theft of sensitive commercial information to manipulate markets	Theft of personally identifiable information to defraud individuals	Data leakage on account of unauthorized access
Recent Examples	WanaCrypt0r ransomware infects organisations via trusted 3rd party application	DDoS attack on DNS provider disrupts internet traffic to orgs like Amazon and PayPal	DDoS attacks aimed at online banking services or time critical price sensitive market data feeds	Malware attack on banks' SWIFT channel or their customers' online banking sessions	Insider theft of proprietary trading algorithms or market sensitive M&A data	Hack of customer web application to access customer database and exfiltrate PII	Customer credit status and transaction information leaked due to unauthorized access

Thematic, Emerging and Sectoral risk will continue to evolve

Thematic security risk	Emerging technology risk	Specific sector risk
Cyber Governance	Internet of Things	Culture and Behavior
Compliance Risk	Cloud	Cyber Resilience
Cyber Risk Management	Block chain	Skills Shortage
External Attacks	Quantum Computing	Payments Systems
Insider Threat	Artificial Intelligence	Web Platforms
Third Party	Algo Trading	Mobile Platforms
Data Security	Augmented/Virtual Reality	Mainframe

Strategic Roadmap adopted by global regulators



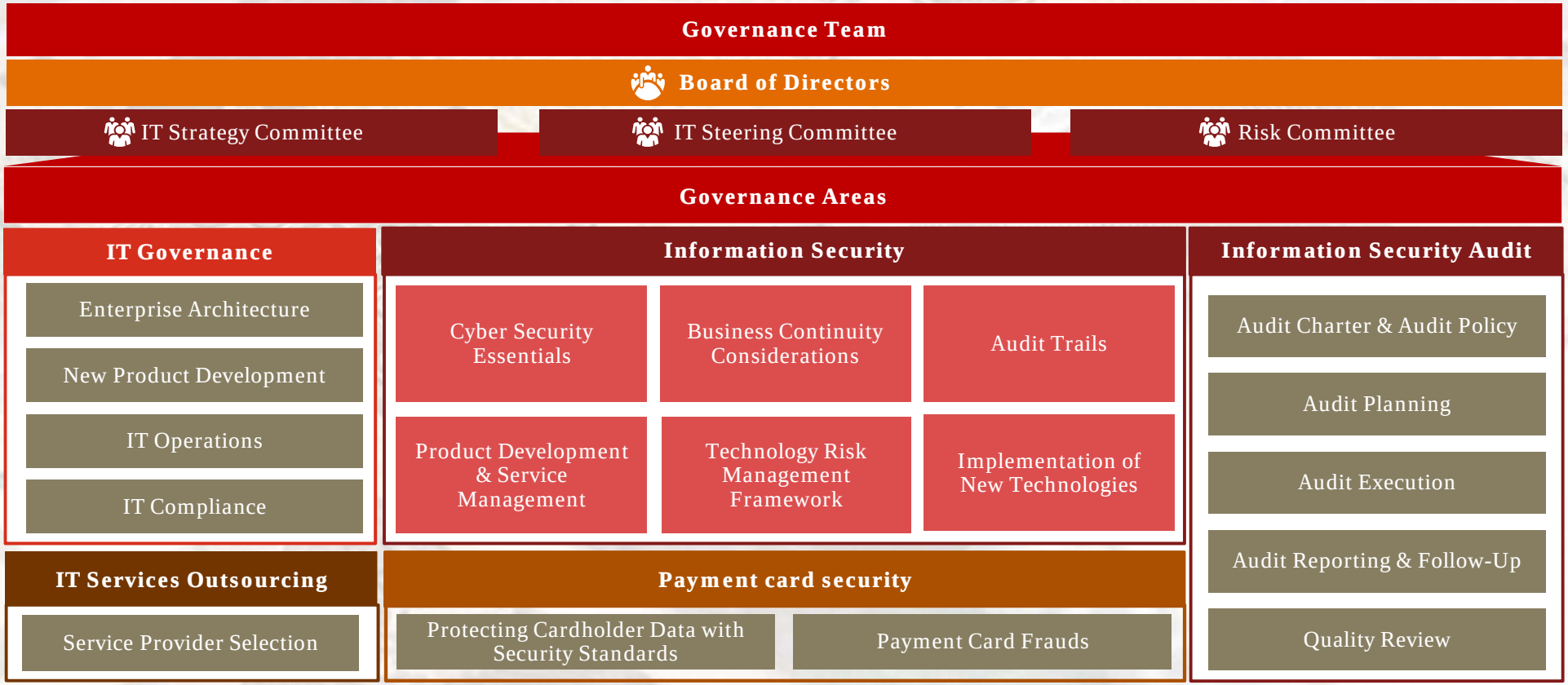
Purpose for Technology Risk Management Guidelines by NBC

PURPOSE

To ensure the Cambodia Banking and Financial Institutions "BFIs" sector contributes to the security and stability of the global financial markets through the implementation of informed supervision and regulation and develops a culture of collaborative sharing of cybersecurity information, knowledge and best practice.

- ***Continuous improvement to address emerging risks***
- ***Inform regulator on the implementation status***
- ***Collaboration within the sector to evolve best practices***
- ***Establish guidelines for the banking sector***

Governance Framework designed by National Bank of Cambodia



Areas within each domain – potential coverage as part of the Risk Management Guidelines

1. Information Technology Governance

1.1. Proposed Structure for IT Governance
1.2. Proposed members for various committees and their roles and responsibilities

2. IT Governance policy and procedures

2.1. IT policy, standards and procedures

3. Information Security Policy and Procedures

3.1. Cyber Security Essential
3.2. Project Development and service management
3.3. Business Continuity considerations
3.4. Audit Trails
3.5. Technology risk management framework
3.6. Implementation of new technologies

3.2. Project Development and Service Management

3.2.1. Change Management
3.2.2. Migration Controls
3.2.3. Incident management

3.1. Cyber Security Essentials

3.1.1. Access Controls
3.1.2. Network Security
3.1.3. Remote Access
3.1.4. Patch Management
3.1.5. Cryptographic Controls
3.1.6. Vulnerability Assessment
3.1.7. Physical and Environmental Security
3.1.8. User Training Awareness
3.1.9. System and Application Security Controls
3.1.10. Data Security
3.1.11. Wireless Security
3.1.12. Supplier Relationship

3.3. Business Continuity Considerations

3.3.1. Business Continuity Planning

3.4. Audit Trails

3.5. Technology Risk Management Framework

3.5.1. Information Security and Information Asset Lifecycle
3.5.2. Cyber Risk Management

3.6. Implementation of New Technologies

3.6.1. Internet Banking
3.6.2. Mobile Banking and e-Wallet
3.6.3. Cloud Computing
3.6.4. SWIFT Security
3.6.5. Security of ATMs and Payment Kiosks

4. IT Services Outsourcing

4.1. Risk Management in outsourcing arrangements
4.1.1. Service provider selection

5. Information Security Audit

5.1. Audit Charter, audit policy to include IS audit
5.2. Planning an IS Audit
5.3. Executing an IS Audit
5.4. Reporting and Follow-up
5.5. Quality review

6. Payment Card Security

6.1. Protecting cardholder data with security standards
6.2. Payment card frauds

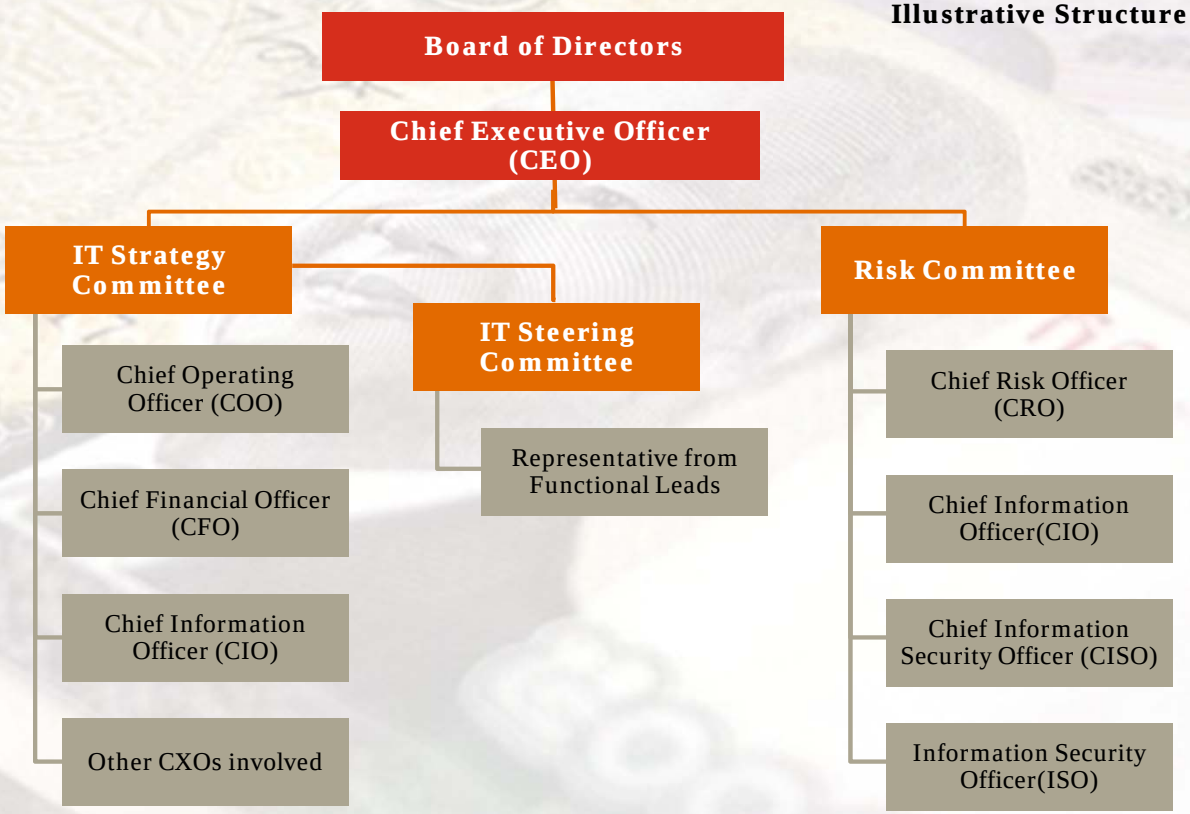
Timelines for Adoption

1. Information Technology Governance

What is required ?

- Define IT governance structure which adequately support business strategies and aim at achieving organizational objectives.
- Define an effective governance process that meets expectations as outlined by the Board
- Monitor the risk position and report to executive management team
- Review the oversight responsibilities on an ongoing frequency
- Provide guidance to prioritize on emerging threats and risks applicable for IT operations

Illustrative Structure



Refer Section 1.1 for details

Board of Directors

Key takeaways

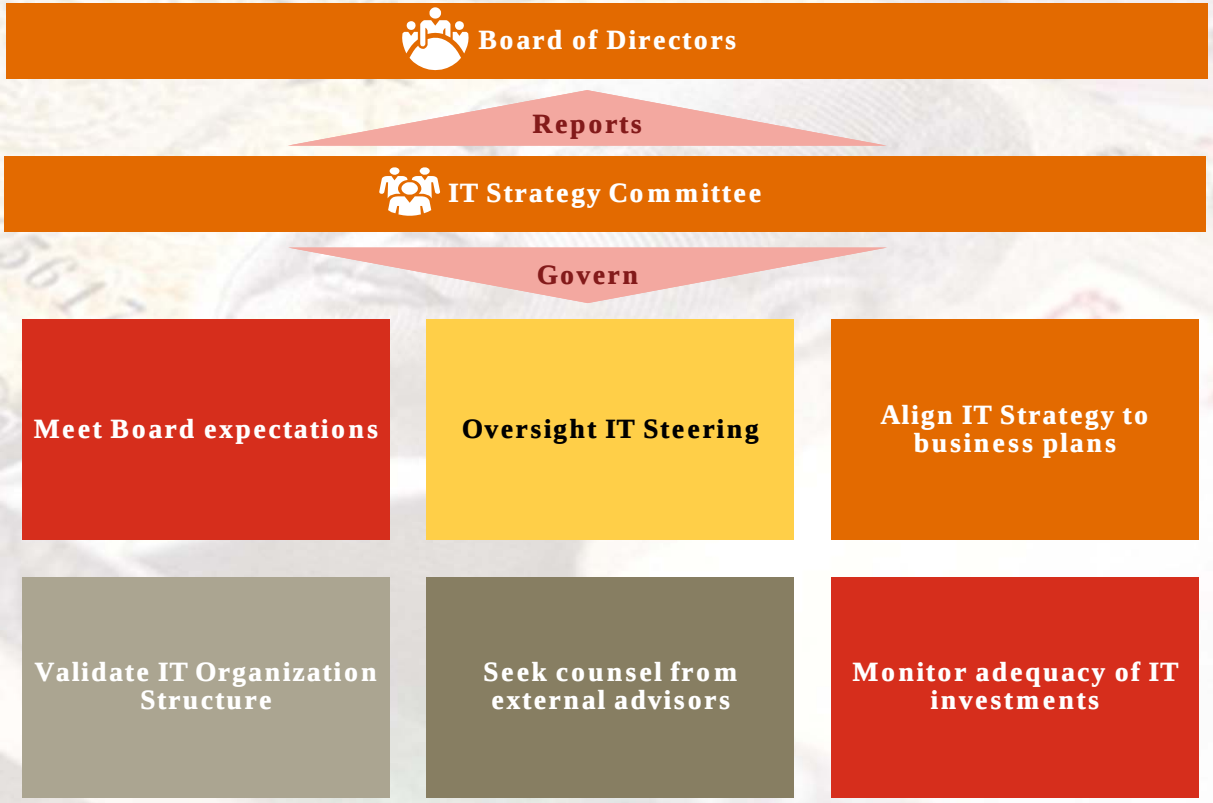
- Ensure IT Governance framework is approved by the Board
- Review performance of IT governance framework
- Review value delivered by IT operations to business
- Monitor on IT investments against the advancements and progress supporting business operations
- Ensure ongoing improvement and effective monitoring of IT risks

Refer Appendix 7.1 and 7.2 for details

IT Strategy Committee

Key takeaways

- Meet Board expectations on delivery of business values
- Oversee performance of IT Steering function
- Align IT Strategy to support business plans
- Validate IT Organization structure and its alignment to meet business expectations
- Seek counsel from external advisors and ensure availability as an when required
- Monitor adequacy of IT investments for ongoing operations and IT risk management

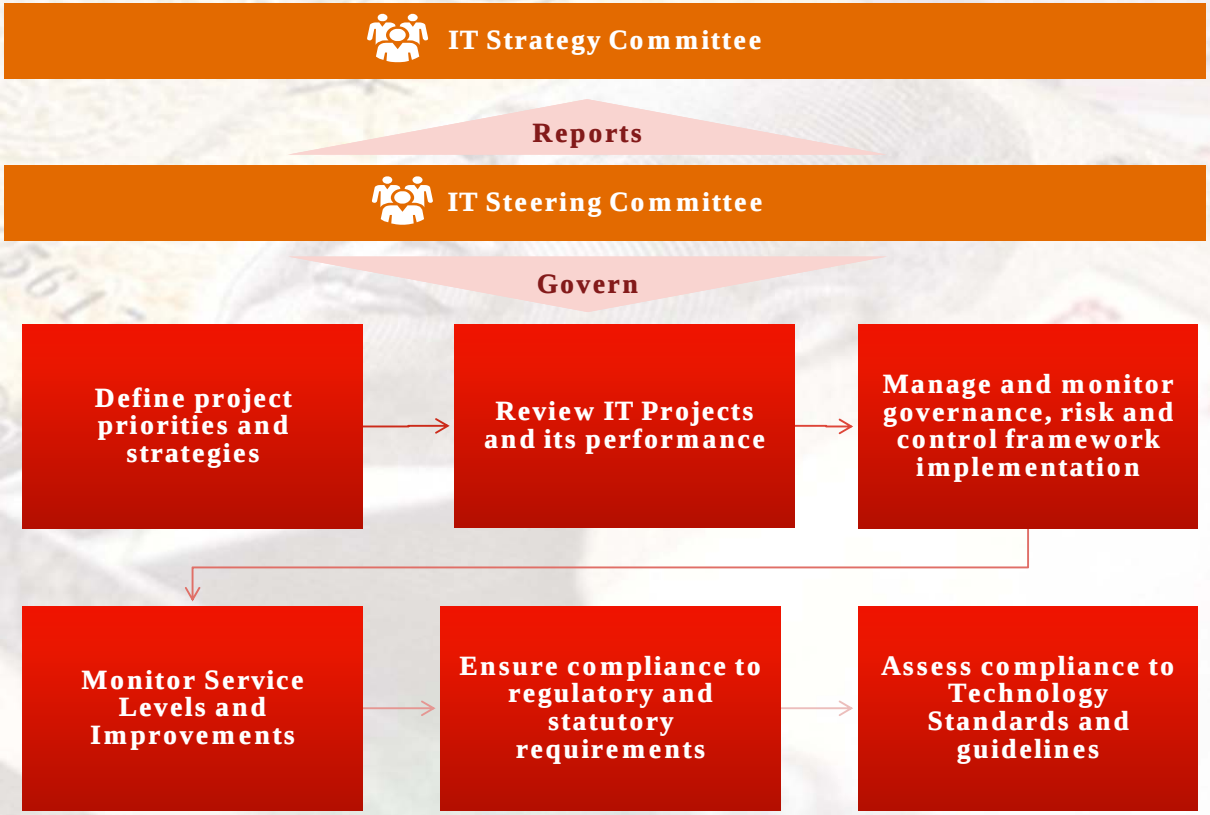


Refer Appendix 7.1 and 7.2 for details

IT Steering Committee

Key takeaways

- Ensure project priorities and strategies are defined to meet to business strategies
- Review IT projects performance for budget overruns and challenges
- Manage and monitor governance, risk and control implementation which support secure IT implementations
- Ensure compliance to regulatory and statutory requirements are met as part of IT implementation
- Assess compliance to technology standards as part of the governance framework



Refer Appendix 7.1 and 7.2 for details

Risk Committee

Key takeaways

- Define effective risk management to achieve data confidentiality, security, reliability, resiliency and recovery across IT organization
- Promote in developing IT-related enterprise risk management expertise
- Establish practices to put robust risk management systems and operating procedures
- Provide updates over implementation of appropriate practices and controls to mitigate risks
- Appraise on environmental, operational and system changes and its impact on risk analysis

2. IT governance policy and procedures

What is required ?

- Identify the nature and scope of technology activities implemented to enable business operations.
- Evaluate the efficiency and effectiveness of IT systems and control environment
- Identify long term strategy for keeping up-to-date with technology developments and systems advancements
- Identify short term initiatives to ensure long term strategy is met
- Define risk management framework for IT operations to identify, track and mitigate risks
- Annually review of IT strategy to account on the organization's business plans and IT environment changes

Enterprise Architecture

New Product Development

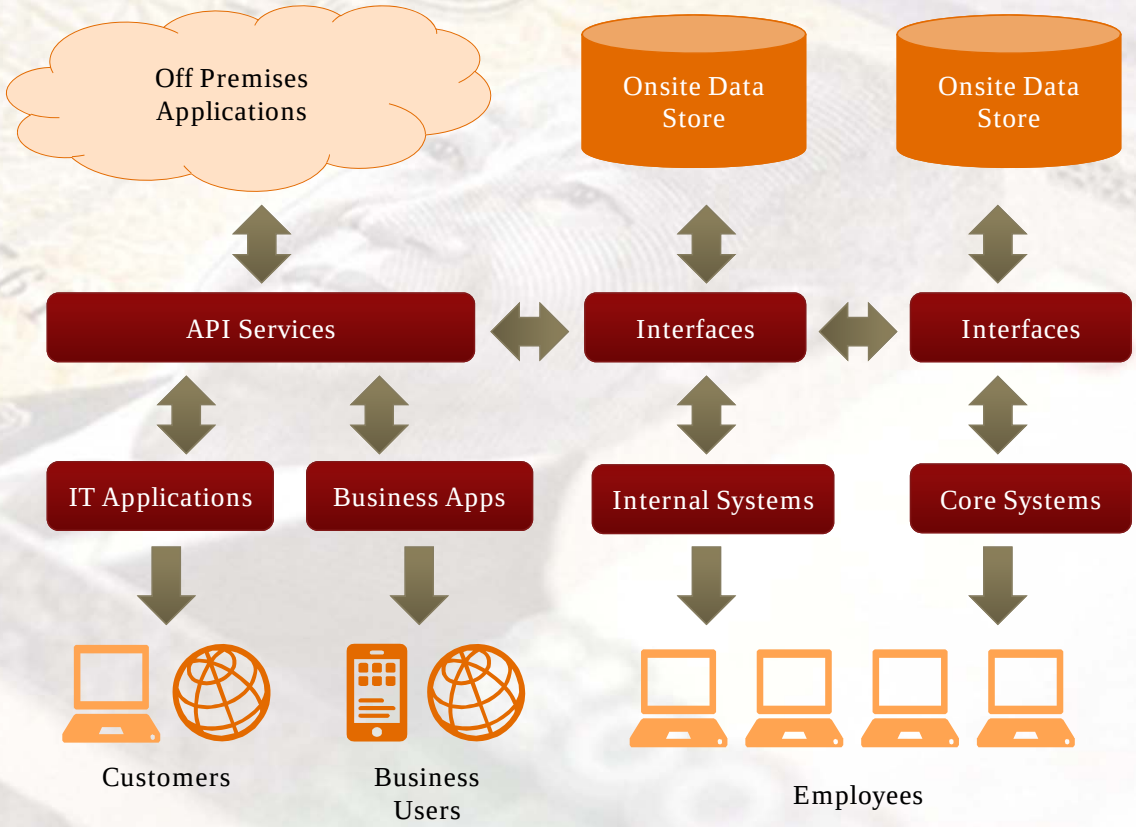
IT Operations

IT Compliance

A. Enterprise Architecture

Key takeaways

- Define organizational roles around individuals managing:
  - Systems
  - Software
  - Network and telecommunication
  - Other technology interventions
- Plan out a strategic plan to enhance enterprise architecture
- Define a technology plan for IT applications and its system components



B. New Product Development

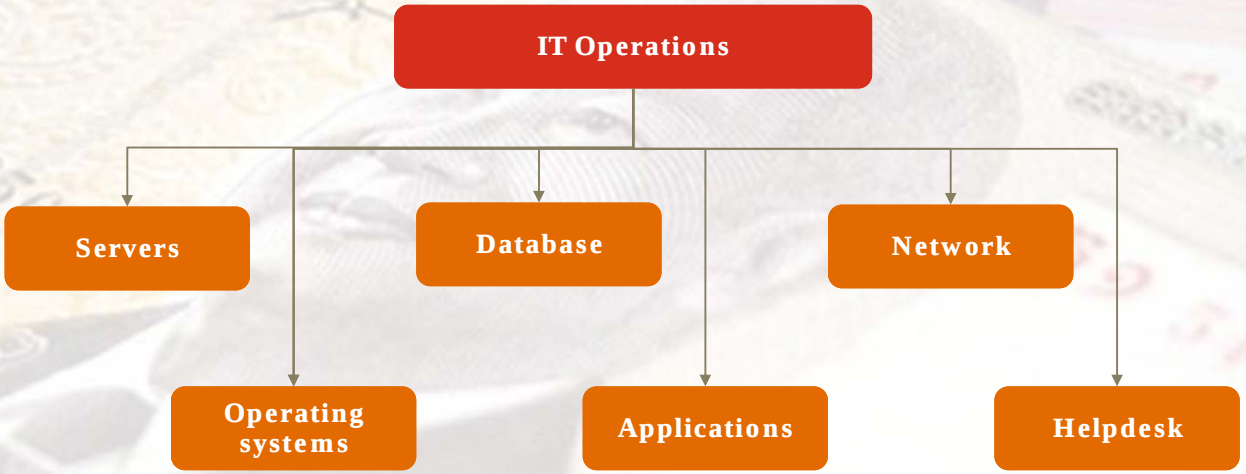
Key takeaways

- Define oversight capabilities on IT initiatives or projects
- Manage budgets and timelines on IT initiatives
- Define project management responsibilities to meet project and functional expectations
- Define responsibilities to manage outsourced IT operations and vendor teams
- Ensure secure development and testing responsibilities for product development before go-live

C. IT Operations

Key takeaways

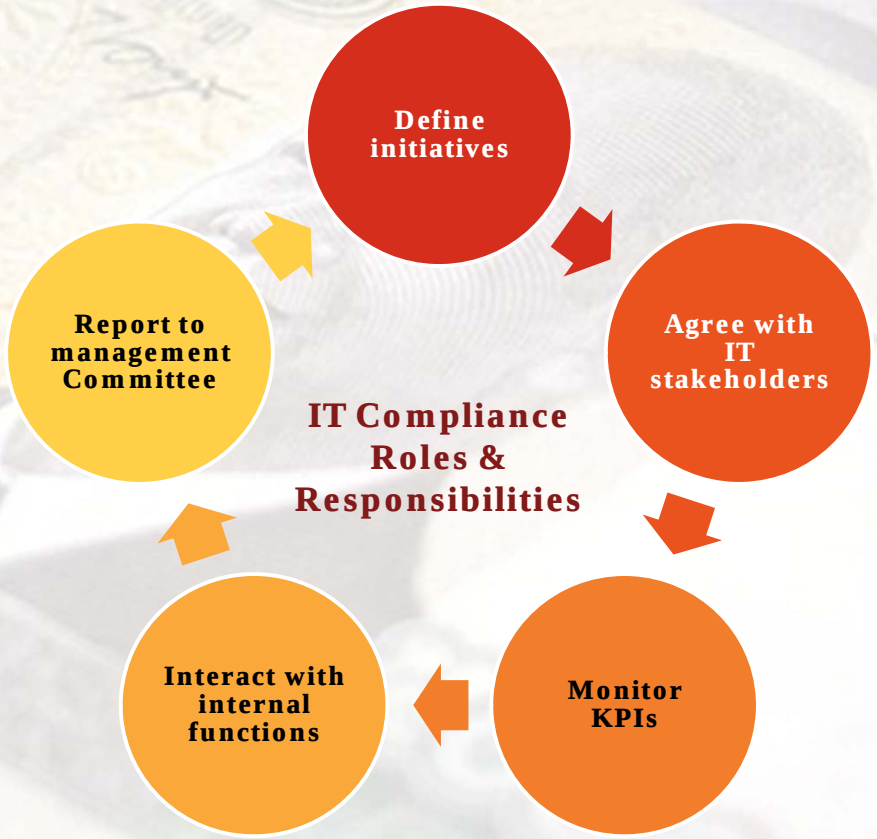
- Set up oversight of all IT processes and systems within organization
- Define roles and responsibilities for team managing systems and operations as follows
    - Servers
    - Operating systems
    - Database
    - Applications
    - Networks
    - IT helpdesk



D. IT Compliance

Key takeaways

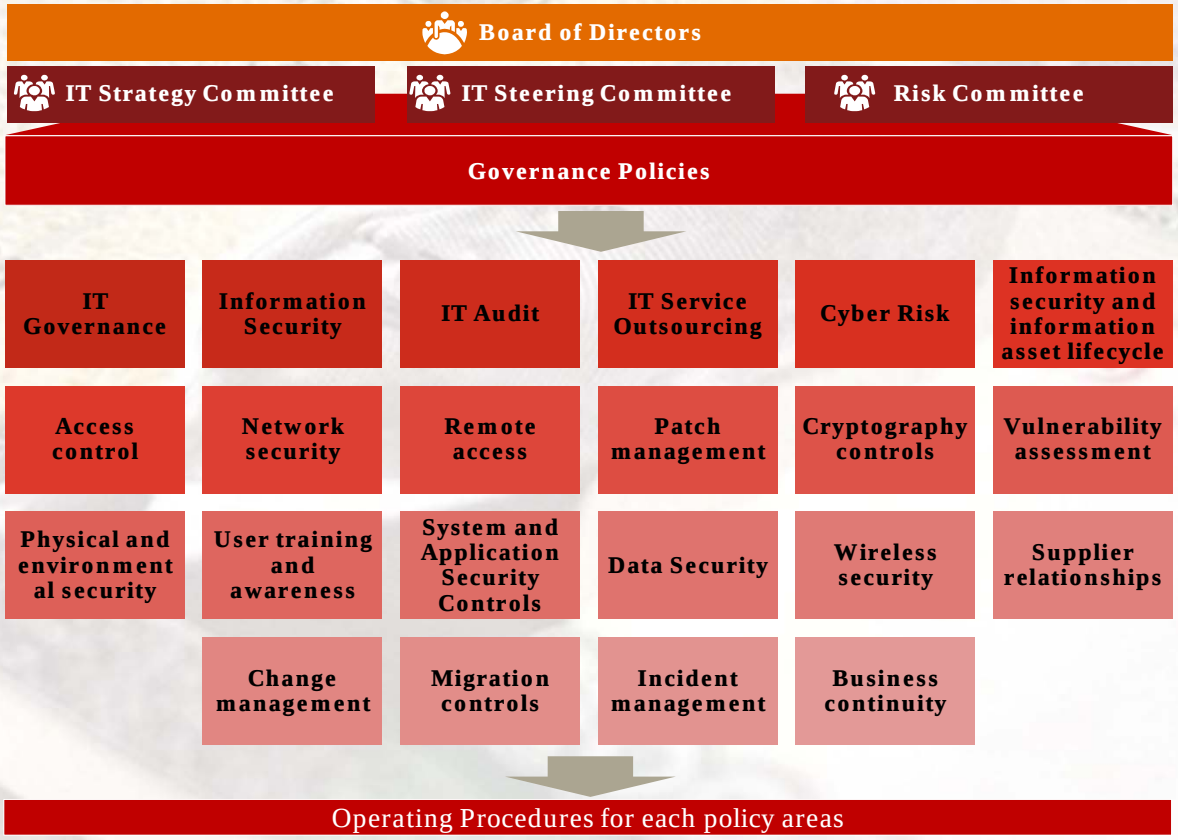
- Define quality, risk and compliance management initiatives within the IT vertical
- Discuss and agree on the key performance indicators with IT operations
- Monitor against the key performance indicators defined
- Provide inputs to various committee for action and reporting
- Interact with audit, risk and compliance functions



2.1 IT Policy, standards and procedures

Key takeaways

- Documenting and rollout of IT Operations policy and procedures duly approved by board
- Document detailed operational procedures for relevant areas in data center operations
- Follow a structured approach for the short-term and long-term planning process
- Review IT strategy and policies as per changes to organization's business plans and IT environment annually
- Set-up standards for IT Infrastructure baselines, Application, system development, enterprise data classification, IT compliance guidelines and risk identification
- Develop training plans for building internal skills of IT manpower



3. Information security policy and procedures

What is required?

- Ensure confidentiality to prevents the disclosure of information to unauthorized individuals or systems
- Integrity of data against unauthorized modifications shall be maintained
- Ensure availability of any information system to serve its business purpose
- Ensure authenticity of data, transactions, communications or documents
- Define controls around non-repudiation to fulfil one's obligations under a contract/transaction
- IT Systems must challenge for identification and authorization to ensure that the requested activity or access to an object is genuine and authorized
- Ensure accountability and auditability of all activities and operations managed by the teams

3.1. Cyber Security Essentials

What is required ?

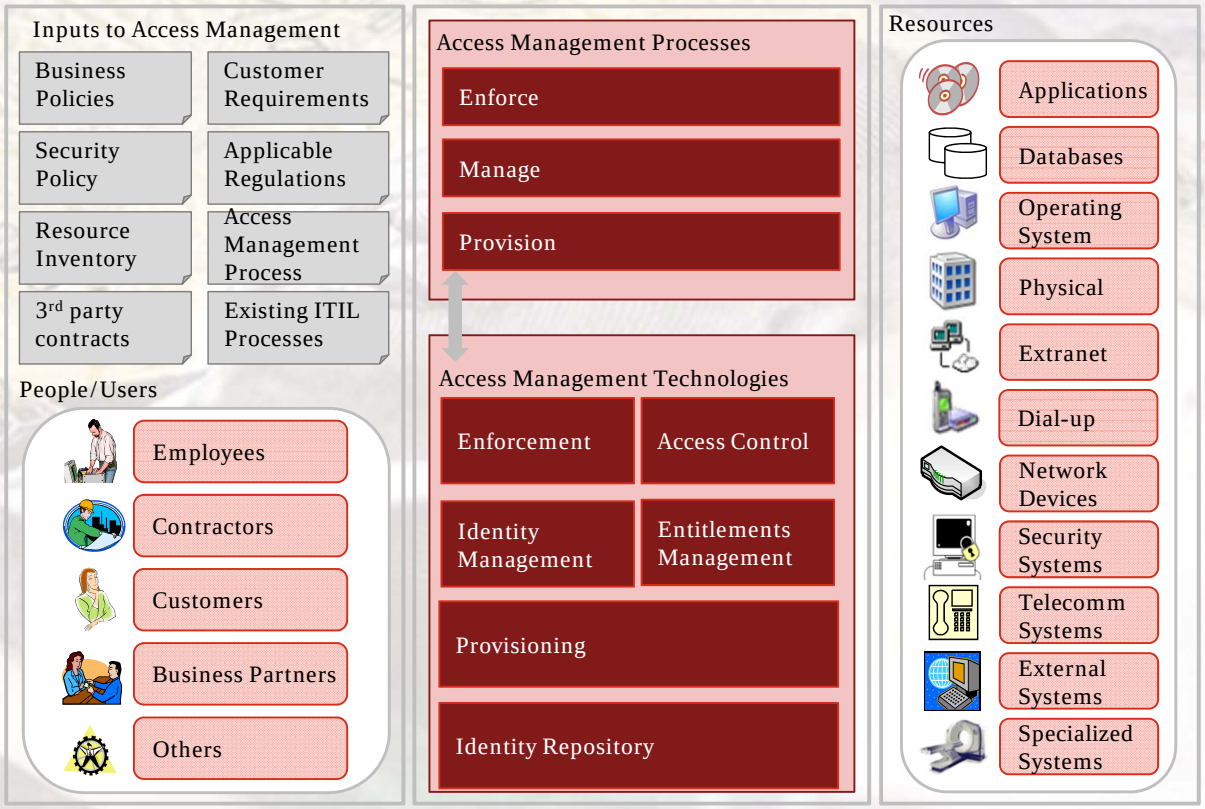
- Assess application and infrastructure implementation within organization against the specified areas
- Perform gap assessment to verify control implementation and maturity across IT landscape
- Define controls as per guidelines requirements and ensure adoption across Application and infrastructure systems
- Formulate policies, standard operating procedures to define operational activities and clear accountability for implementation, monitoring and management

Access control	**Network security**	**Remote access**
Patch management	**Cryptography controls**	**Vulnerability assessment**
Physical and environmental security	**User training and awareness**	**System and Application Security Controls**
Data Security	**Wireless security**	**Supplier relationships**

3.1.1. Access Control

Key takeaways

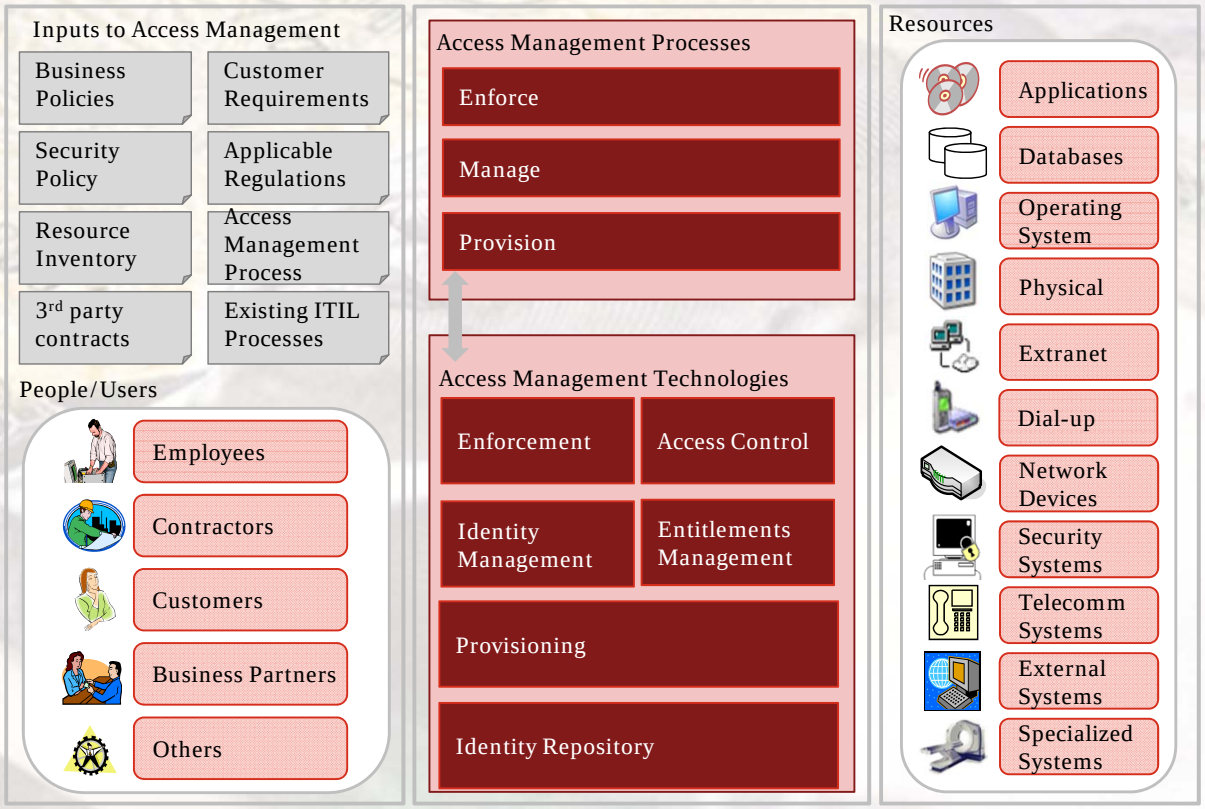
- Define user life cycle including purpose and period of access for all users including privileged users and vendors
- Implement strong password policy and controls for user access to applications, networks and databases.
- Ensure that logs for user access and system logs are maintained for audit and forensic purposes and are encrypted
- Implement multi factor authentication for users that connect using internet, non trusted devices, third party premises
- Develop access control policy to monitor and regulate the use of all IT assets
- Ensure that access should be provisioned on need to know basis and should follow least privilege principle



3.1.1. Access Control (Contd...)

Key takeaways

- Ensure end to end integration of the user lifecycle through a centralized system
- Ensure that user identity should be common across systems
- Privileged user should have differential techniques for authentication
- Define approval matrix and escalation matrix throughout the lifecycle
- IDAM should form a central/common user id repository



3.1.2. Network Security

Key takeaways

- Prepare network diagram that includes all the major components of the IT infrastructure
- Define different network zones based on the business function and criticality. (E.g. Third party zone, server zone, DMZ etc.)
- Assess the risks associated with Wireless Local Area Network before deployment
- Implement redundancy for all critical devices
- Complete backup of configuration should be taken on periodic basis
- Network service agreements to consider the Security mechanisms, service levels and management requirements
- Security features of network services
- Conduct regular enforcement checks to ensure that the baseline standards are adhered to

Network Deployment

- Network diagram
- Install and configure network security devices
- Standard Operating Procedures for installation and configurations
- Security baselines

Secure Network Configuration

- Interfaces configuration/ VLAN
- Ethernet switching
- Routing

Network Security Management and Maintenance

- Security Policy
- Threat mitigation
- VPN configuration
- NAT
- Signature updates
- Firewall rule adjustments
- Licenses
- OS version upgrade
- Adjust routing

Network Monitoring

- Logs and reports
- Data and application activity
- Topology view
- Network failure recognition
- High availability
- Hardware

3.1.3. Remote Access

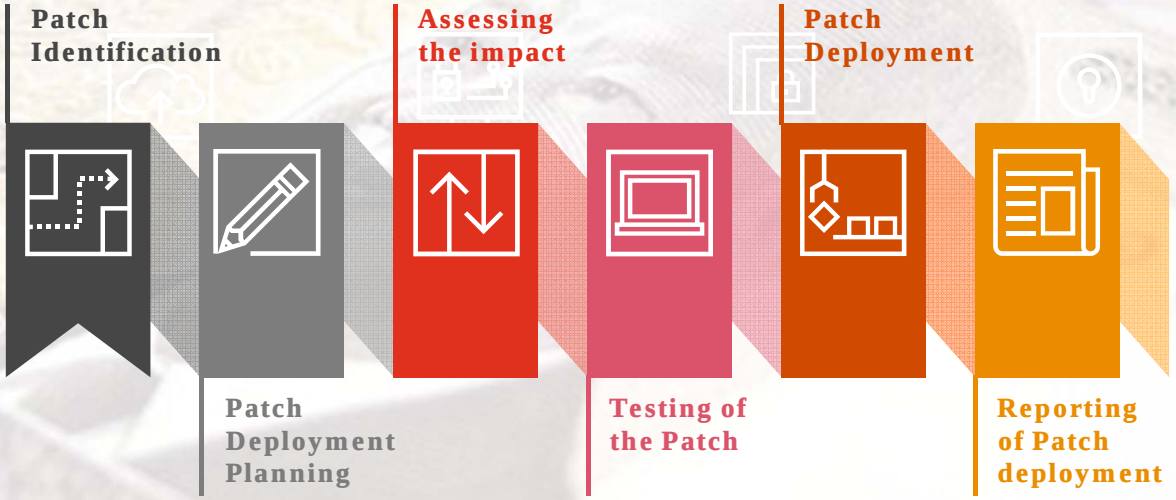
Key takeaways

- Remote access policy and provision on compelling business requirement and regular review of the remote access approval
- Securely configure remote access devices
- Use encryption to protect communication channels to restrict the risks related to network spoofing
- Establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure
- Adequate logging and monitoring of remote access to be enforced
- Enforce two-factor authentication process
- Restrict remote access through modems. If required, consider the following:
    - Enable modems for specific and authorized external requests
    - Configure modems to not answer inbound calls

3.1.4. Patch Management

Key takeaways

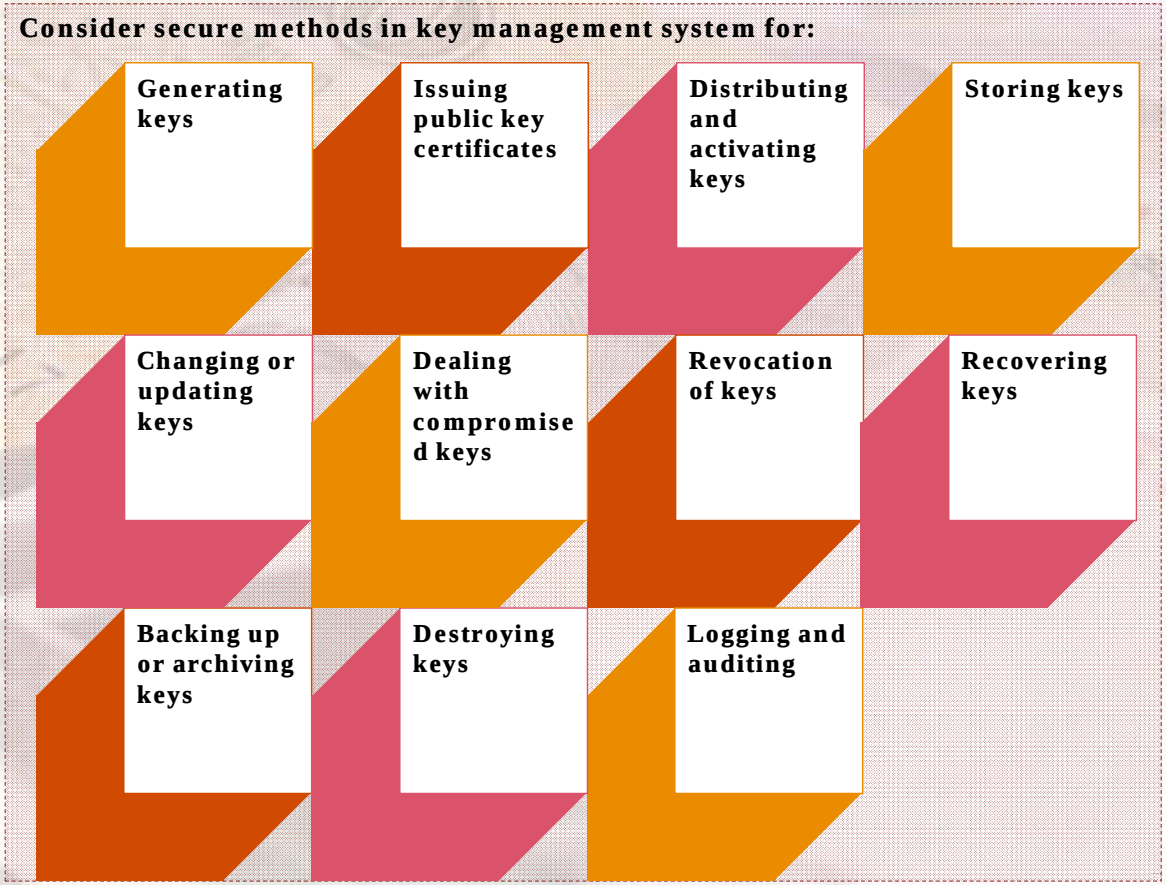
- Establish patch management procedure to identify, categorize and prioritize the security patches
- Implementation of security patches in timely manner
- Critical patches to be evaluated in a test environment prior to deployment in production systems
- Validate patches to ensure the patch is from an authorized source
- Assessment of business impact due to implementation of patches
- Reporting on the status of patch deployment
- Alternative methods to be established in case of failure of deployment of security patch
- Consider deployment of automated patch management tools and software update tools for all systems



3.1.5. Cryptography controls

Key takeaways

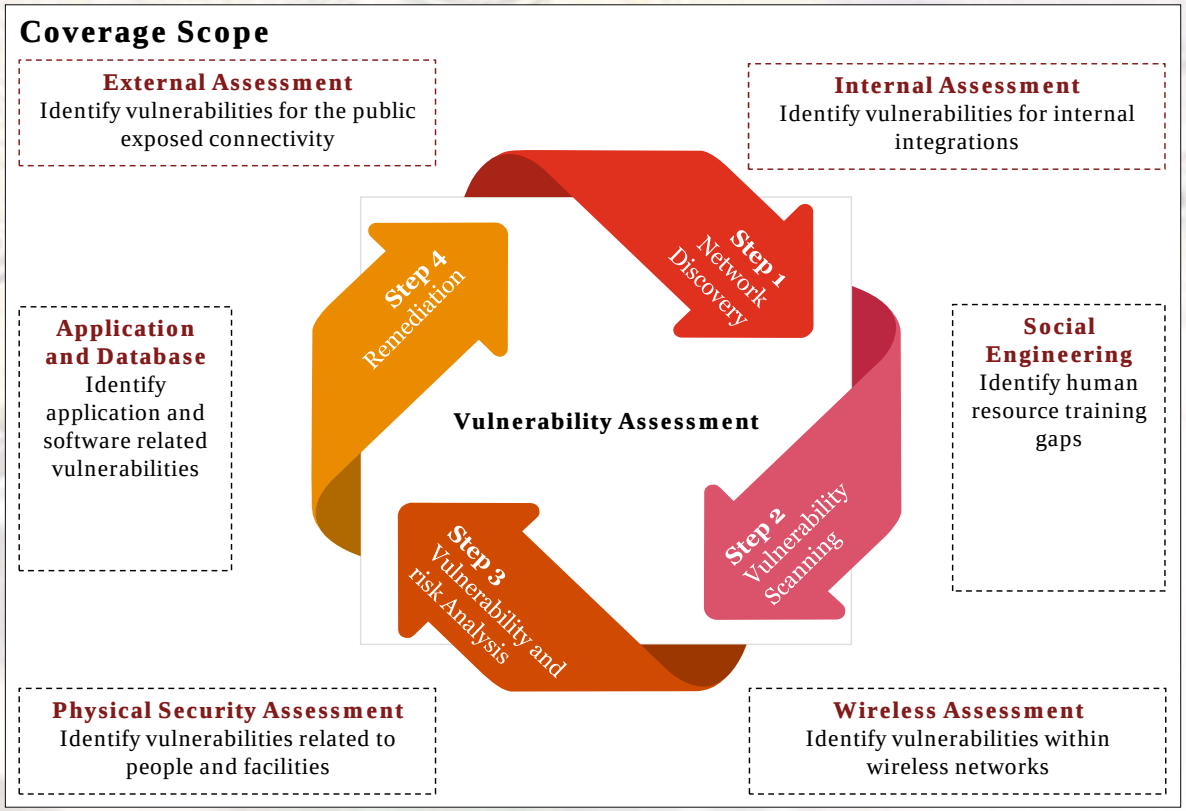
- Risk based analysis to identify the required level of protection taking into account the type, strength and quality of the encryption algorithm required
- Establish policy document to include requirements for managing cryptographic keys through their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys
- Cryptographic algorithms, key lengths and usage practices to be selected according to best practice
- Protection of cryptographic keys against modification, loss, unauthorized use, disclosure and to be physically protected
- Implementation of secure methods for key management system
- Establish key management systems based on an agreed set of standards, procedures and secure methods for following:



3.1.6. Vulnerability Assessment

Key takeaways

- Deployment of combination of automated tools and manual techniques to perform a comprehensive VA on a periodic bases
- For in-depth evaluation of security posture of system, penetration tests to be conducted at least annually
- Establish to remediate the issues identified in VA & PT and perform subsequent revalidation of the remediation
- Perform vulnerability scanning in an authenticated mode at period intervals
- For repeated vulnerabilities, to be addressed by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk
- Provide status updates regarding the number of unmitigated, critical vulnerabilities, for each department/division, and plan for mitigating to senior management on a periodic basis.



3.1.7. Physical and environmental security

Key takeaways

- Deployment of environmental controls for
  - Secure locations of critical assets
  - Restrict access to sensitive areas
  - Monitoring mechanisms for the detection of compromises of environmental controls
- Implement controls for secure storage of media
- Controls to be implemented:
  - limit access to media
  - Physical protection against natural disasters, malicious attack or accidents
  - labelling, and logged access
  - limiting access by means of physical locks, keypad, passwords, biometrics, etc.

Physical and Environmental Security Controls

Site/ facility design considerations
- Security Survey
- Site planning
- Crime prevention through environmental design
- Location threats
- Man-made threats
- Utility concerns

Internal Security
- Doors and Locks
- Turnstiles and mantraps
- Keys, locks and safes
- Key control
- Biometrics
- Windows, Glass, Garages

Perimeter Security
- Defence in depth
- Gates and fences
- Perimeter Intrusion Detection
- Lighting
- Access Control
- Closed circuit TV
- Guards
- Design requirements

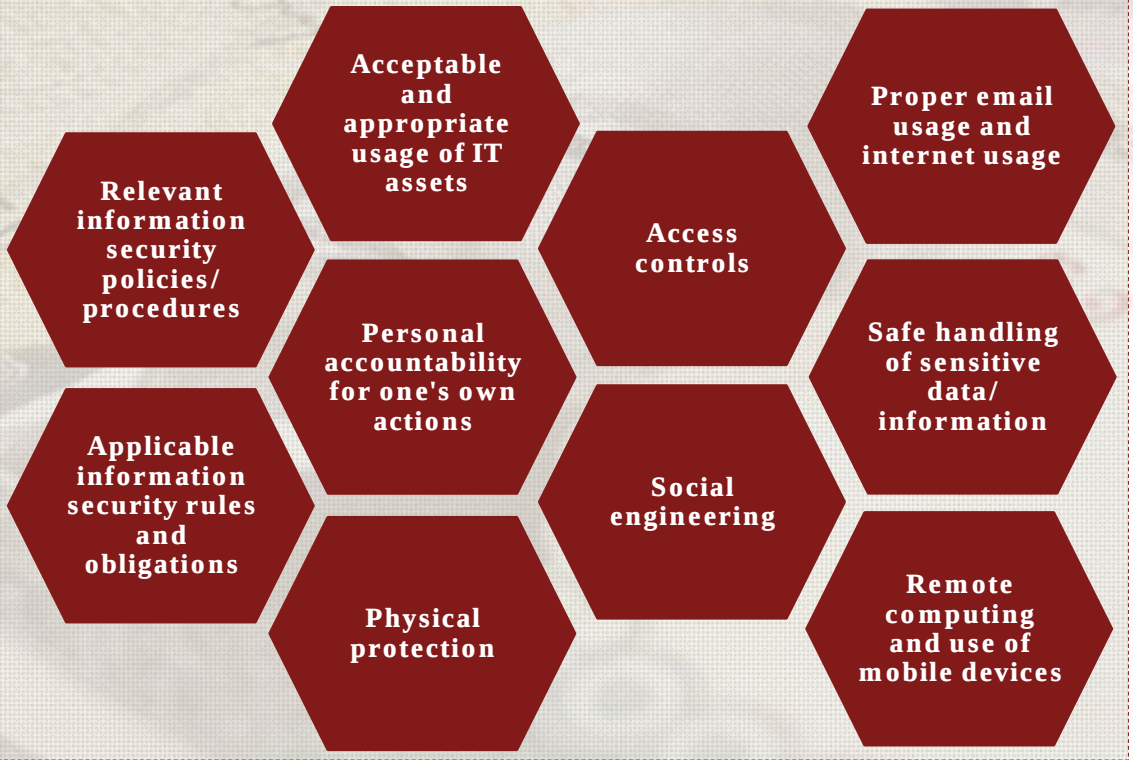
Facilities Security
- Escort and visitor control
- Secure operational area
- Environment controls
- Power supply
- HVAC
- Water

3.1.8. User training and awareness

Key takeaways

- Conduct awareness training for the organization's personnel covering IT policy, processes and procedures
- Include Cyber Security Awareness program as a human resource initiative
- Utilize internal communication channels, facilities and technologies to promote good security practice
- Social engineering based intervention to test awareness levels
- Measure effectiveness of awareness programs and evolve to improve effectiveness
- Maintaining records of education, training, skills, experience and qualifications

Key areas for user awareness programme:



3.1.9. System and application security controls

Key takeaways

- Assign the role for application owner to be the concerned business function that uses the application
- Application systems to be tested before going live
- Conduct source code review for all critical applications at a minimum after every major patch update
- Exercise due diligence in ensuring its applications have appropriate security controls
- Implementation of recovery measures, user access and data protection controls
- Audit trails for all application systems
- Robust System Security Testing
- Define access control policy for restricting the access to application system

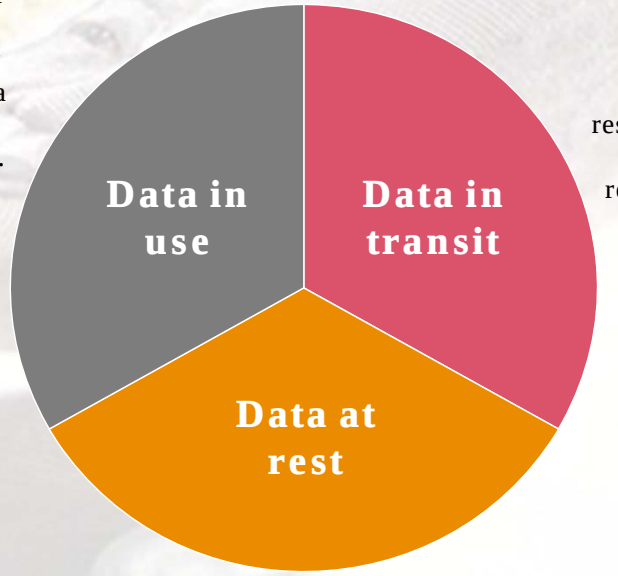
3.1.10. Data Security

Key takeaways

- Define data protection requirements including sensitivity of considering Personally Identifiable Information "PII", organization specific and legal & regulatory requirements
- Perform data discovery to identify storage of sensitive data sets
- Perform data flow analysis to identify movement of sensitive data
- Define rules sets to protect and detect sensitive data sets while enforcing compliance with industry regulations and data protection standards
- Use encryption technologies to encrypt all sensitive data at rest, in transit or on cloud
- Define process to restrict unauthorized data storage
- Block access to known file transfer and e-mail exfiltration websites
- Define disposal procedures for both electronic and paper based media
- Establish a process to continuously mature Data Leak Prevention "DLP" processes

Data in Use:

Active data under constant change stored physically in databases, data warehouses, spreadsheets, etc.



Data in Transit:

Data that is traversing a network or temporarily residing in system memory to be read or updated

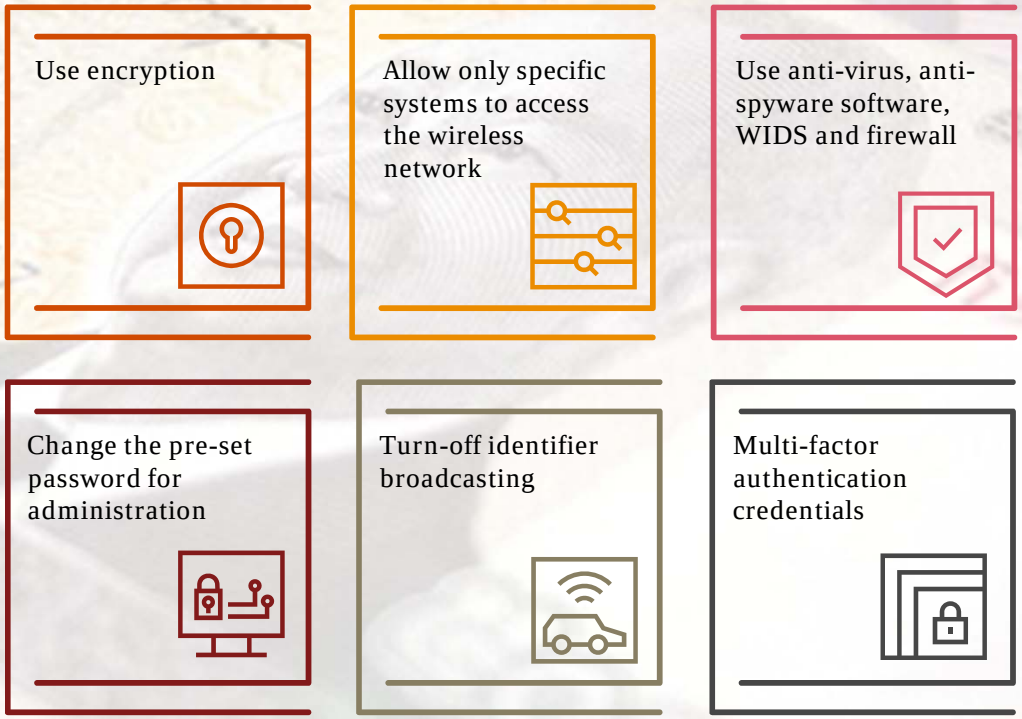
Data at rest:

Inactive data stored physically in databases, data warehouses, spreadsheets, archive, tapes, off-site backups, etc.

3.1.11. Wireless security

Key takeaways

- Provision of wireless access on basis of strong business case
- Establish controls to safeguard the confidentiality and integrity of data passing over wireless networks
- Allow access through authorized devices to shield the internal network from the external risks
- Use strong authentication for access point and device identification
- Monitor rogue access points and devices trying to connect to wireless networks
- Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices, detect attack attempts and successful compromise
- Ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection
- Use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access



3.1.12. Supplier relationships

Key takeaways

- Define supplier governance involving roles and responsibilities, risk identification, risk assessment methodology, risk tolerance levels, escalation matrix and exception requirements
- Classify supplier relationship to prioritize third party stratification of critical vendors and establish contractual terms
- Perform pre on-boarding due-diligence process
- Enforce Non-Disclosure Agreement while dealing with sensitive data
- Conduct regular assessments for periodic reporting to management
- Ensure that service provider adhere to all legal and regulatory requirements of the country
- Establish mechanism to monitor and review the service level delivered
- Define risk dashboard for overseeing health report including recommendations for improvements

3.2. Project Development and Service Management

What is required ?

- Define change management process to streamline implementation of product changes and upgrades securely
- Develop migration policy which documents guidelines on requirement analysis, planning and methodology baselines and sign-off requirements
- Formulate incident management which define guidelines to identify and misuse of computing assets, information disclosure or events
- Define Standard Operating Procedures establish the operational activities, clear accountability and communication strategies

3.2.1. Change Management

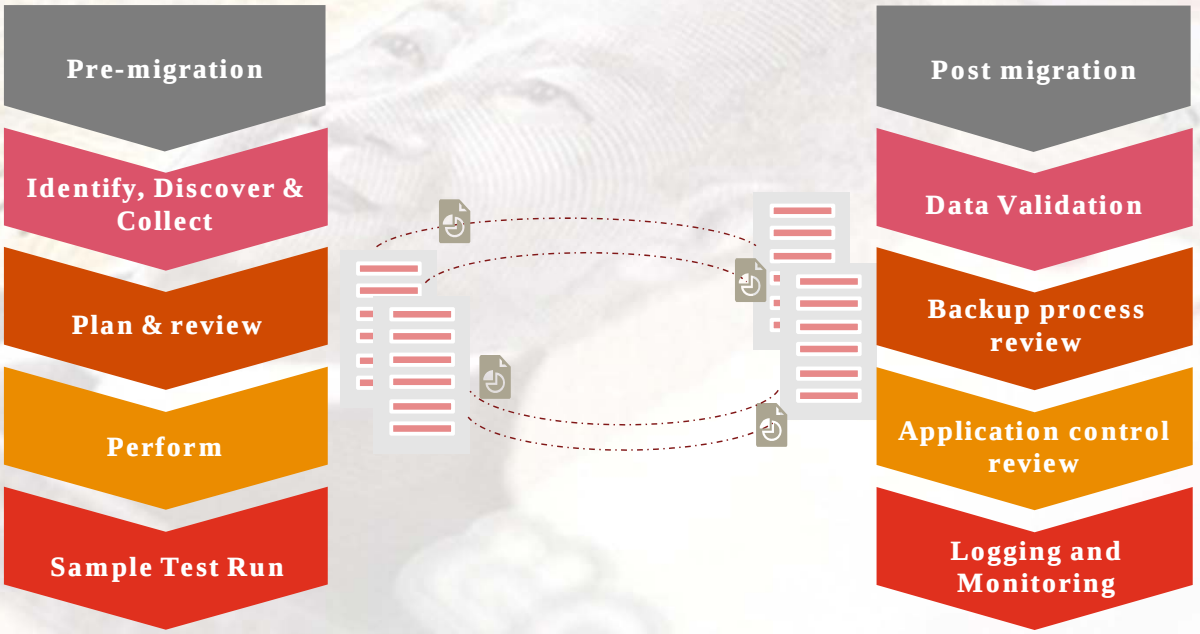
Key takeaways

- Establish change management process to ensure changes to production systems are deployed in a controlled manner
- Conduct risk and impact analysis of changes prior to deployment in production environment
- Develop and document appropriate test plans and approval of all changes to the production environment by personnel delegated
- Perform backups of affected systems or applications prior to the change
- Establish alternative recovery options to address situations where a change does not allow the BFI to revert to a prior status
- Incorporate controls in case of exception based and emergency changes
- Ensure that the logging facility is enabled to record activities that are performed during the migration process

3.2.2. Migration controls

Key takeaways

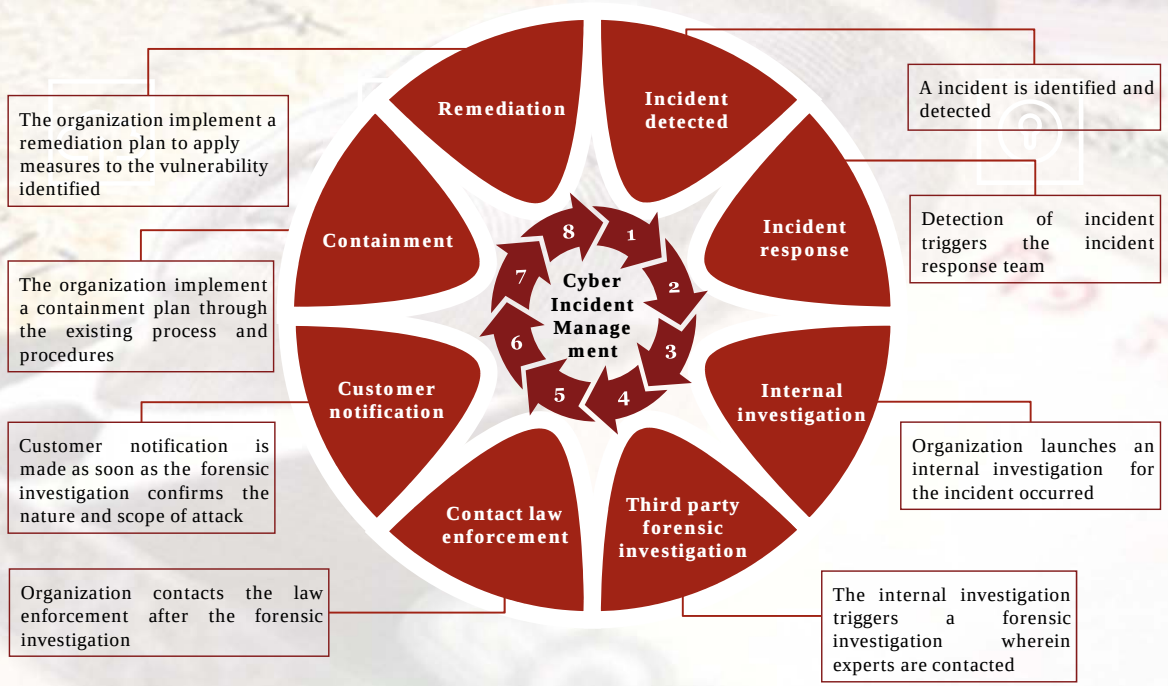
- Key aspects to considered include completeness, availability of data backup, integrity of data, consistency of data and continuity
- Perform a pre-implementation review of application controls, including security features and controls over change management process
- Conduct post implementation review of application controls
- Conduct detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system
- Conduct a review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system
- Availability of error logs pertaining to the pre-migration/migration/post migration period along with root cause analysis



3.2.3. Incident Management

Key takeaways

- Develop, implement and refine processes for preventing, detecting, analyzing and responding to information security incidents
- Establish escalation and communication processes and lines of authority
- Establish the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
- Develop a process to communicate with internal parties and external organizations
- Classify IT incidents into different severity levels based on the business impact and urgency of the incident
- Integrate information security incident response plans within the organization's disaster recovery and business continuity plan
- Organize, train and equip teams to respond to information security incidents



3.3. Business Continuity Considerations and Planning

What is required ?

- Establish a business continuity management framework for managing cyber risks by defining the teams, setting up operating process and reporting structure
- Identify and classify critical business assets as per their business criticality
- Identify applicable threats along with impact and consequences for each applicable scenarios
- Implement a robust response team which can identify, analyse, protect and report in a timely manner
- Install appropriate mechanisms to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements
- Plan communication strategy to assist with a coordinated and effective media statements and strategic media outreach

Incident Response Plan

Focuses on the **immediate response** and should include **people safety and protection of assets** at site level

Business Recovery Plan

Focuses on **knowledge and actions** required to recover business operations and maintain services following a disruption

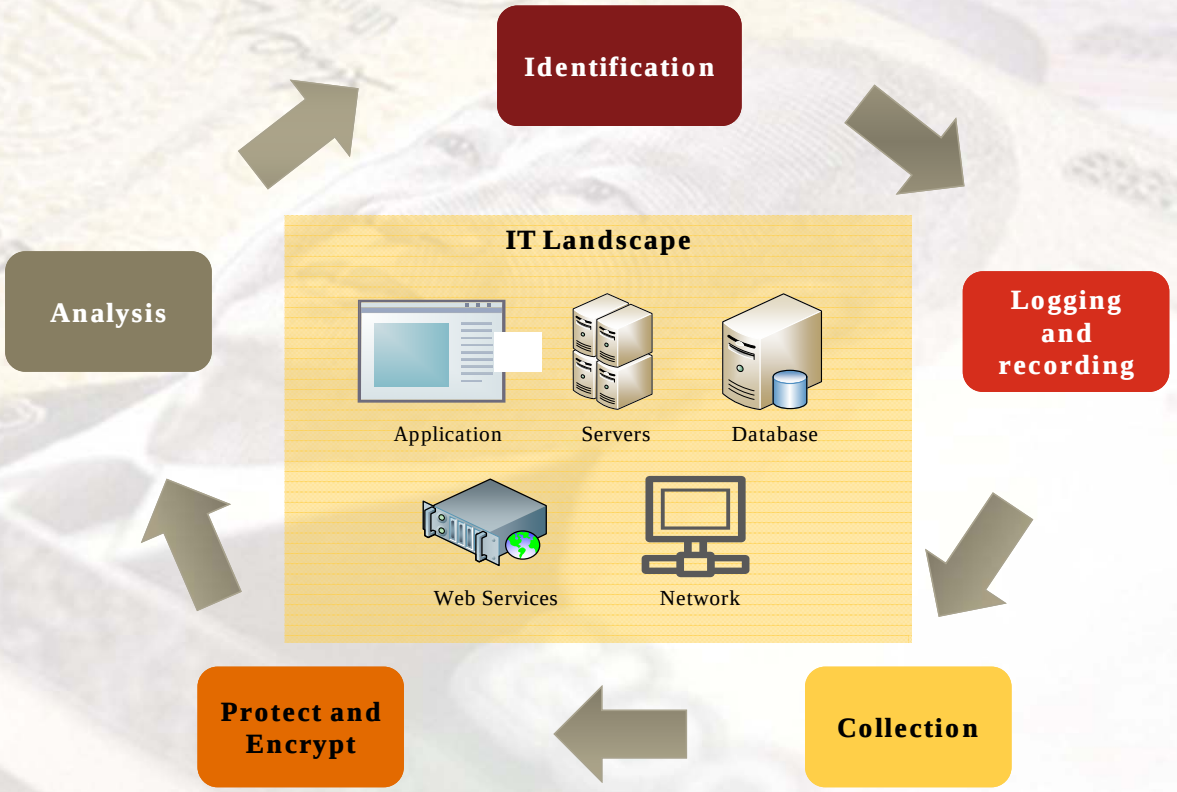
Crisis Management Plan

Focuses on **leadership and coordination** of the response to address business impacts, including communications with business stakeholders

3.4. Audit Trails

What is required ?

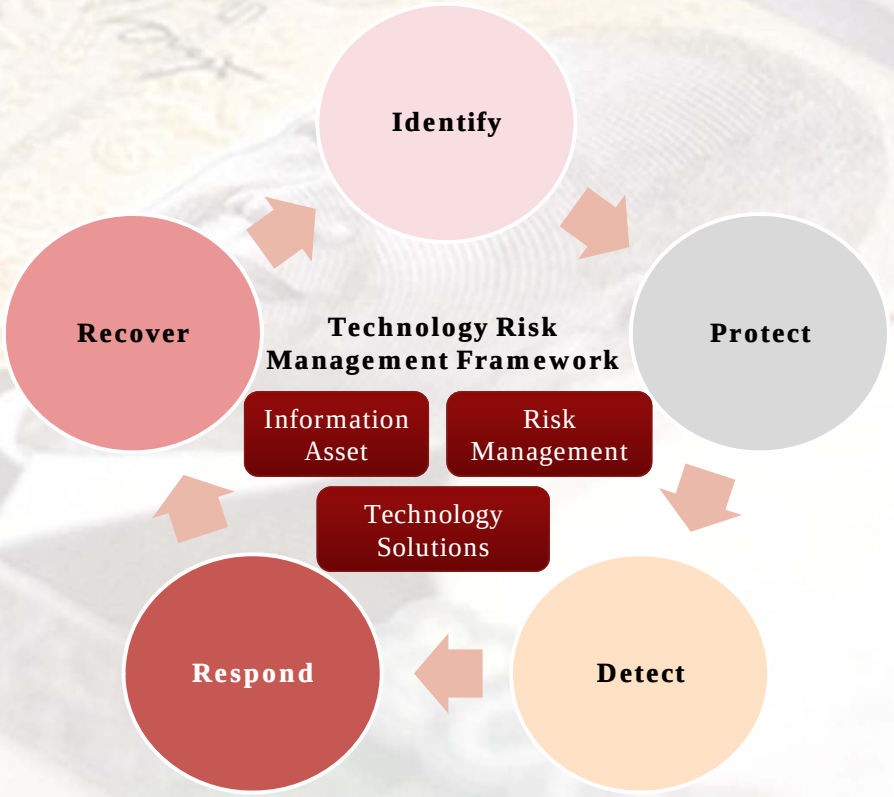
- Ensure audit logging mechanisms are developed for each application and infrastructure components
- Identify whether the logs capture user activities, exceptions, faults and information security events
- Ensure that the audit logs have restricted access to authorized individuals to avoid log data modification or alterations
- Ensure retention of audit trails are in line with business, regulatory and legal requirements
- Formulate process around reviewing audit logs for unauthorized activities and operations



3.5. Technology risk management framework

What is required ?

- Define effective risk management practices and internal controls to achieve data confidentiality, system security, reliability, resiliency and recoverability
- Classify Information Assets as per degrees of sensitivity and criticality in meeting business objectives
- Define roles and responsibilities of the personnel who play a vital role throughout the risk management lifecycle
- Develop process and technology capabilities around the principles of identification, detection, protection, response and recovery.



3.5.1. Information security and Information asset lifecycle

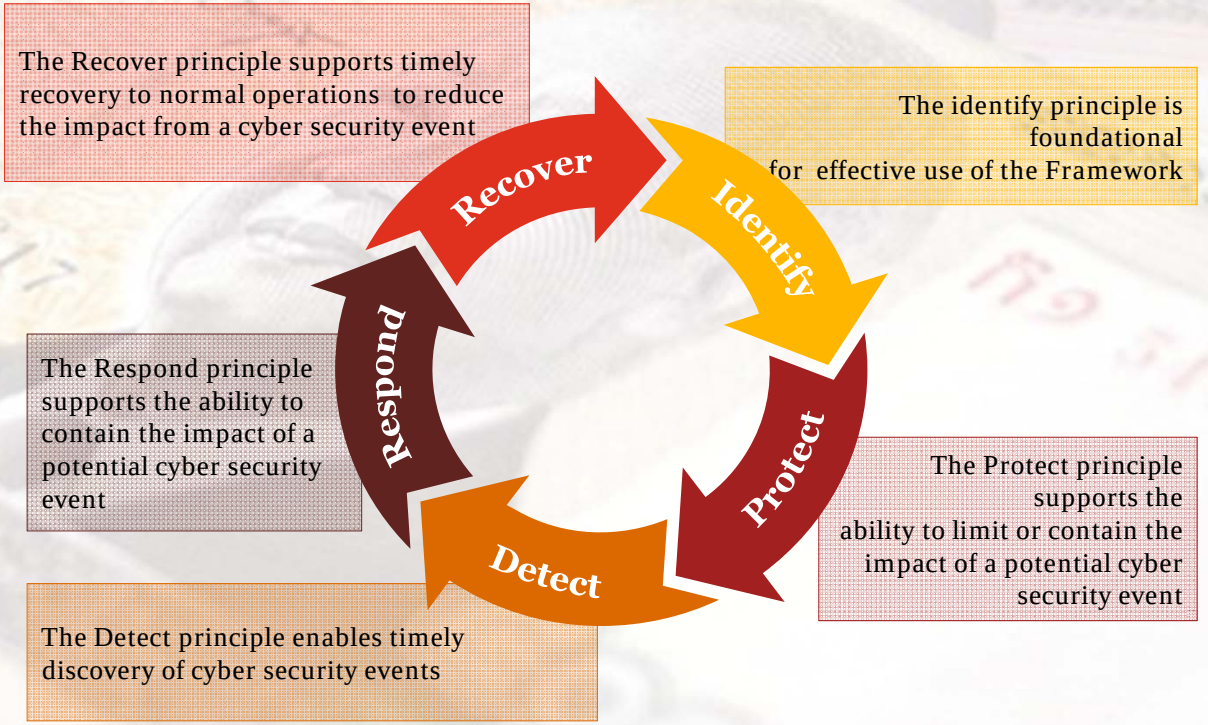
Key takeaways

- Plan and design controls to ensure that information security is embodied in the overall information systems architecture and the implemented solutions
- Acquisition of new assets and all existing assets should be inventoried
- Information assets are classified as per varying degrees of sensitivity and criticality to meet business objectives
- Classification of information helps reduces the risk and cost of over- or under- protecting information resources in aligning security with business objectives
- Ongoing support and maintenance controls would be needed to ensure that IT assets continue to meet business objectives
- Define roles and responsibilities of the personnel who play a vital role throughout the information asset lifecycle.
- Decommissioning and destruction controls should be defined to ensure as IT assets reach the end of their useful life

3.5.2. Cyber Risk Management

Key takeaways

- Understand the risk tolerance to prioritize cyber security activities, enabling organizations to make informed decisions about cyber security expenditures.
- Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cyber security programs
- Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities
- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- Develop and implement the appropriate activities to identify the occurrence of a cyber security event
- Develop and implement the appropriate activities to take action regarding a detected cyber security event
- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.



3.6. Implementation of New Technologies

What is required ?

- Identify compliance requirements for new technologies
- Assess the technologies implementation as per the industry specific standards
- Identify applicable business and compliance risks for specific technologies and operations
- Define control mechanisms to detect, monitor and minimize such risks

3.6.1. Internet Banking Security

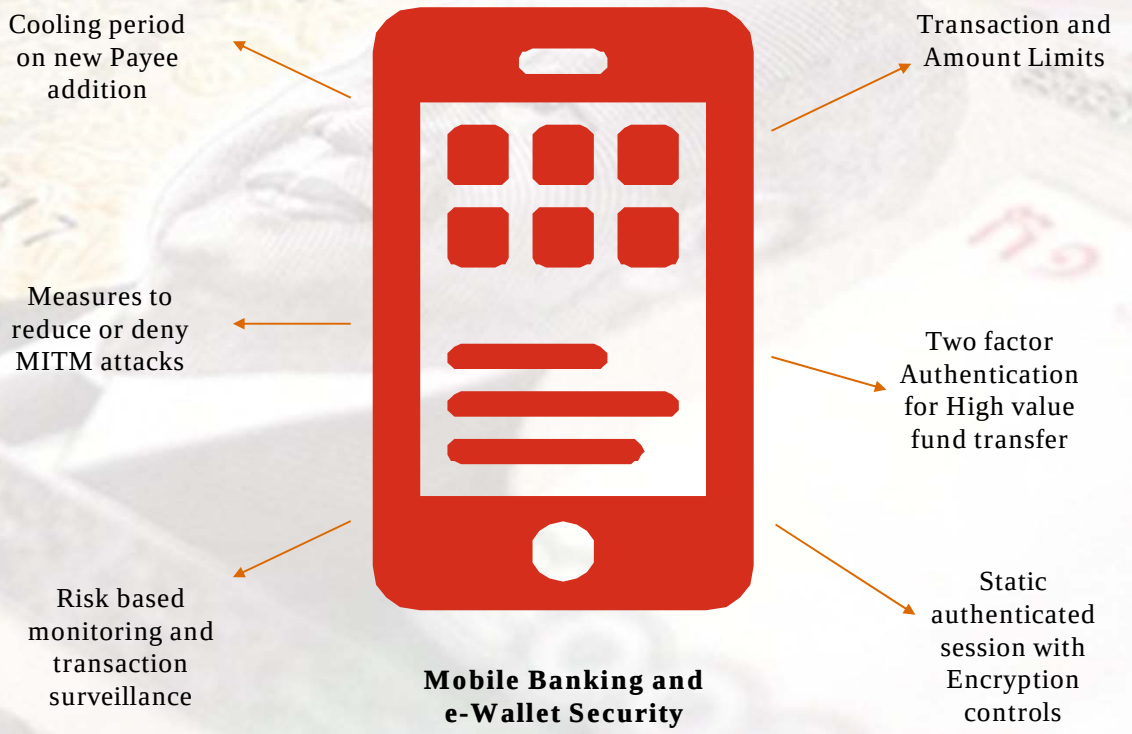
Key takeaways

- Develop a risk mitigation approach for implementing suitable measures for protecting web application
- Ensure suitable security measures for web applications and take reasonable mitigating measures against various web security risks
- Implement well established encryption controls considering the degree of confidentiality and integrity required
- Build network & system monitoring capabilities to detect Denial of Service attacks
- Ensure application doesn't store sensitive information at client side
- Regularly assess information security vulnerabilities and evaluate effectiveness of IT Security risk management framework
- Ensure any new session requires normal user identification, authentication, and authorization

3.6.2. Mobile Banking and E-wallet security

Key takeaways

- Set up daily transaction and amount limits on payments processed for each customer
- Implement two factor authentication for high value fund transfers
- An authenticated session using encrypted protocols should remain intact. In case of any interference, the session shall be terminated
- A cooling period needs to be implemented for any new payee added. The customer needs to be notified over email/SMS for such addition
- A risk monitoring and surveillance process needs to be implemented to monitor fraudulent use
- Implement appropriate measures to minimize exposure to a man-in-the-middle attack (MITM), man-in-the-browser (MITB) attack or man-in-the-application attack



3.6.3. Cloud Computing

Key takeaways

- Verify reputation, history and sustainability of a cloud service provider prior to engagement
- Enterprise to seek regulatory approval prior to hosting cloud services in different geographic location
- Contractual agreement with the cloud service provider should capture trans-border data flows, business continuity requirements, log retention, data confidentiality, data retention and audit trails requirements
- Business continuity and disaster recovery plans must be well documented in line with cloud provider
- Incident management controls for the data hosted in the cloud should be drafted with cloud service providers

3.6.4. SWIFT Security

Key takeaways

- Assess SWIFT systems against compliance requirements mandated by SWIFT service providers
- Restrict access of SWIFT systems and environments from general network environment
- Assign access to infrastructure and applications on the "Need to know" and "Need to have" basis
- Integrate System and infrastructure with Risk Monitoring and surveillance systems to identify anomalies activities, transactions and detect frauds

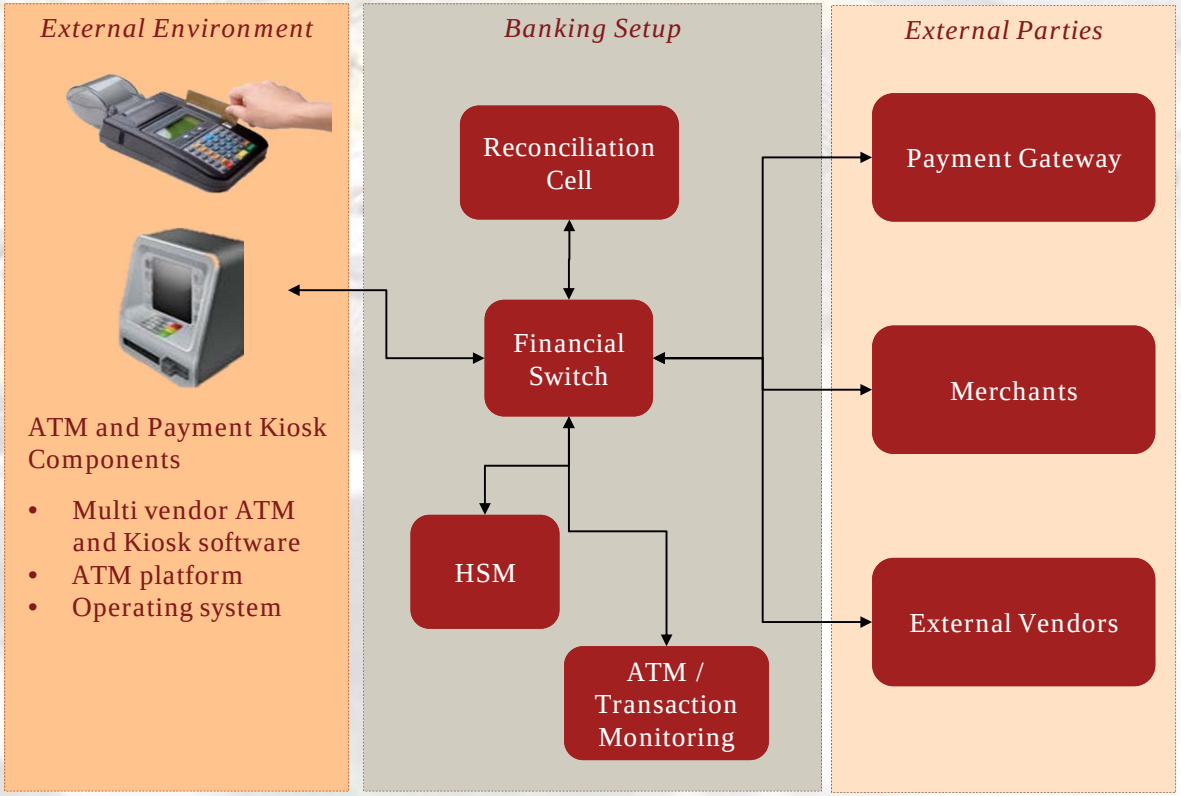
SWIFT Security Objectives

3 Key Objectives	8 Principles
Secure your environment	1. Restrict internet access 2. Protect critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment
Know and limit access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges
Detect and Respond	7. Detect anomalous activity to system or transaction records 8. Plan for incident response and information sharing

3.6.5. Security of ATMs and payment kiosks

Key takeaways

- Install Anti Skimming solutions to detect presence of foreign devices on the ATMs and Payment Kiosks
- Install fraud detection mechanisms to alert appropriate staff on any anomalies observed
- Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission
- Appraise customer over shoulder surfing methods and implement controls on ATM and Payment Kiosks to prevent them
- Conduct high quality video surveillance of activities at these ATM machines and kiosks



4. IT Services Outsourcing

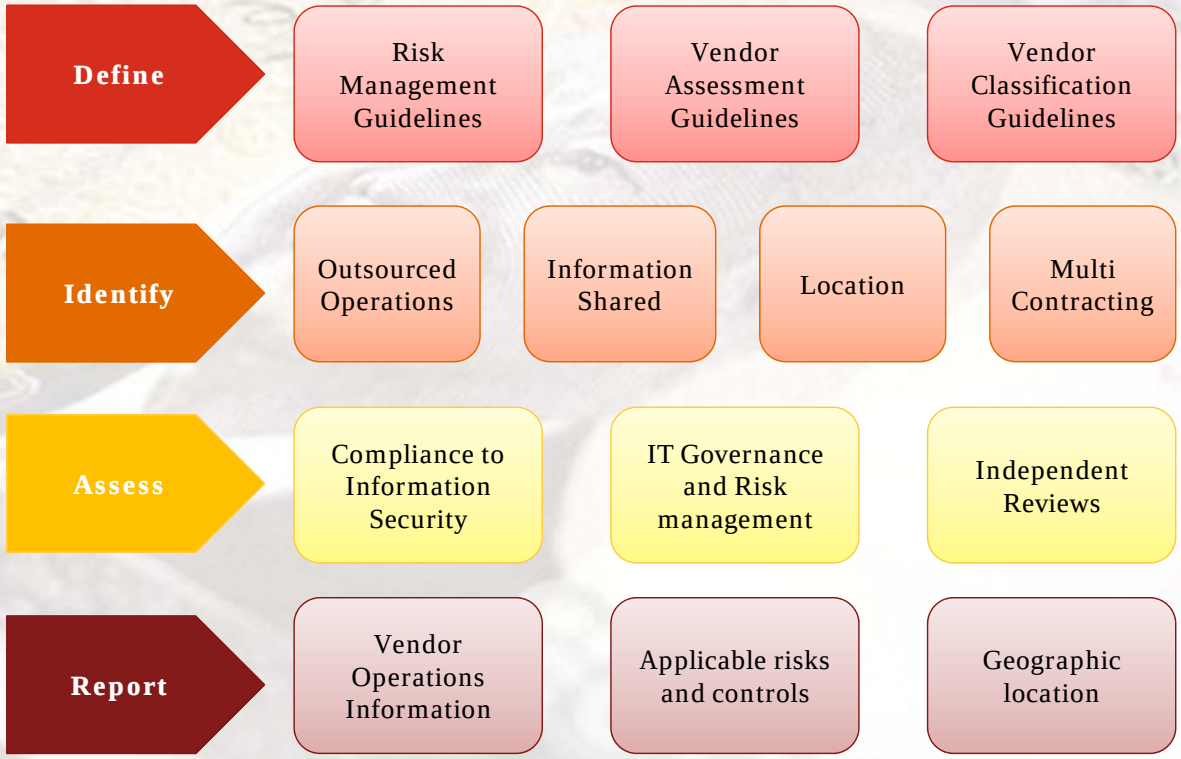
What is required ?

- Define risk management practices to identify, measure and monitor risks applicable to business operations along with outsourcing risks.
- Perform ongoing due diligence for business and IT operations prior to or after onboarding vendors
- Identify and classify service providers based on business criticality and risk vectors
- Report on the business and IT operations outsourced to regulators
- Perform assessments to identify and monitor multiple Service provider relationships on regular intervals
- Key considerations while signing the outsourcing agreement must include due diligence, maintaining caution lists and scoring for service providers (bureau services) and reporting to the regulator

4.1. Risk Management in Outsourcing arrangements

Key takeaways

- Define guidelines and processes around due diligence to evaluate all information of service providers around qualitative, quantitative, financial, operational and reputational requirements
- Engage bureau services to obtain independent reviews and market feedback to supplement internal findings
- Identify multi-contract vendors relationship to understand and monitor the control environment across all vendors
- Report to regulators on scale and nature of functions outsourced, data sharing involved and location wherein the data is stored/processed



5. Information Security Audit

What is required ?

- Document clear mandates on purpose, responsibility, authority and accountability for operating on the Audit Principles
- Formulate an audit programme to evaluate IT risk management practices, its internal control systems and compliance to governance policy framework
- Conduct regular assessments to locate security vulnerabilities and identify corrective actions
- Prepare an audit summary covering opinion on effectiveness of IT control environment and control weaknesses identified
- Review the audit process framework, methodology, tools and techniques based on learnings and shortcomings identified as part of audit assessments

Audit Charter & Audit Policy

Planning an IS Audit

Executing IS Audit

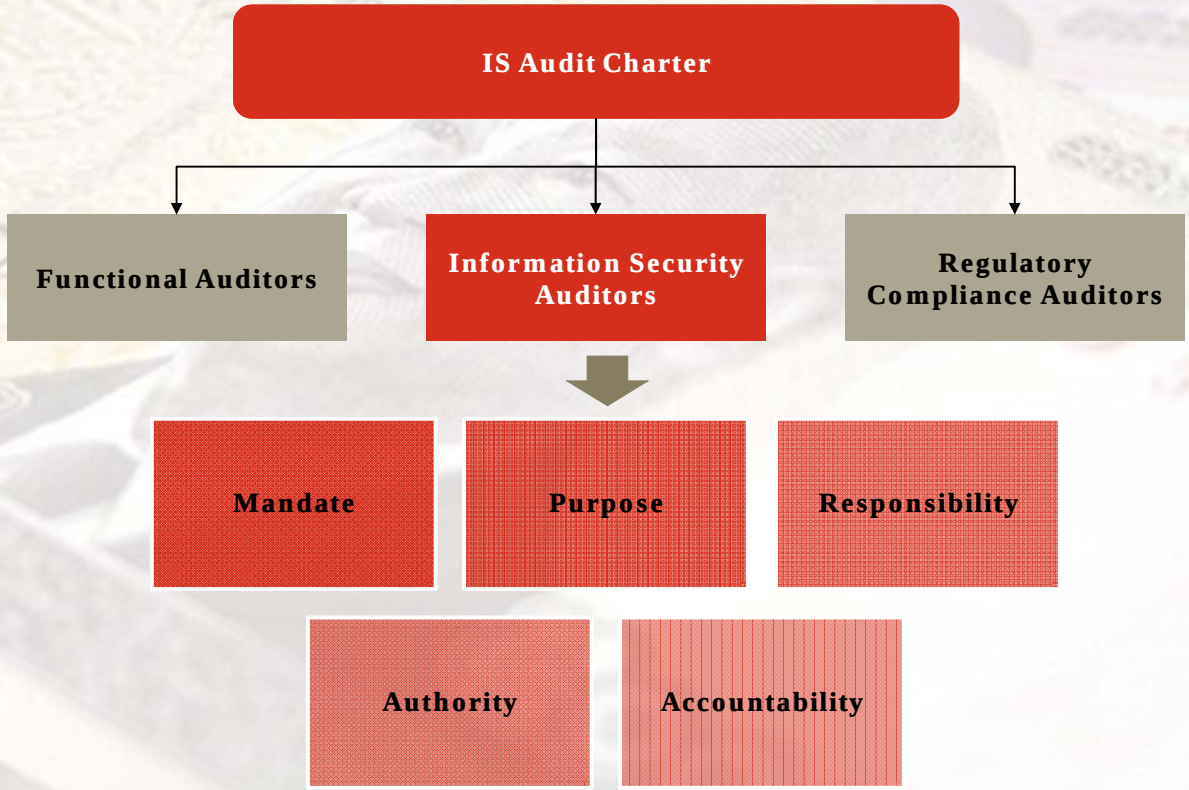
Reporting and follow up

Quality Review

5.1. Audit charter, audit policy to include IS Audit

Key takeaways

- Document audit charter which defined the mandate, purpose, responsibility, authority and accountability of IS Audit members
- IS auditors to adopt the guidelines as defined in the audit charter
- Ensure how the implementation of IS audit standard is adopted and improved on to ensure proper opinion is communicated to the audit committee



5.2. Planning an IS Audits

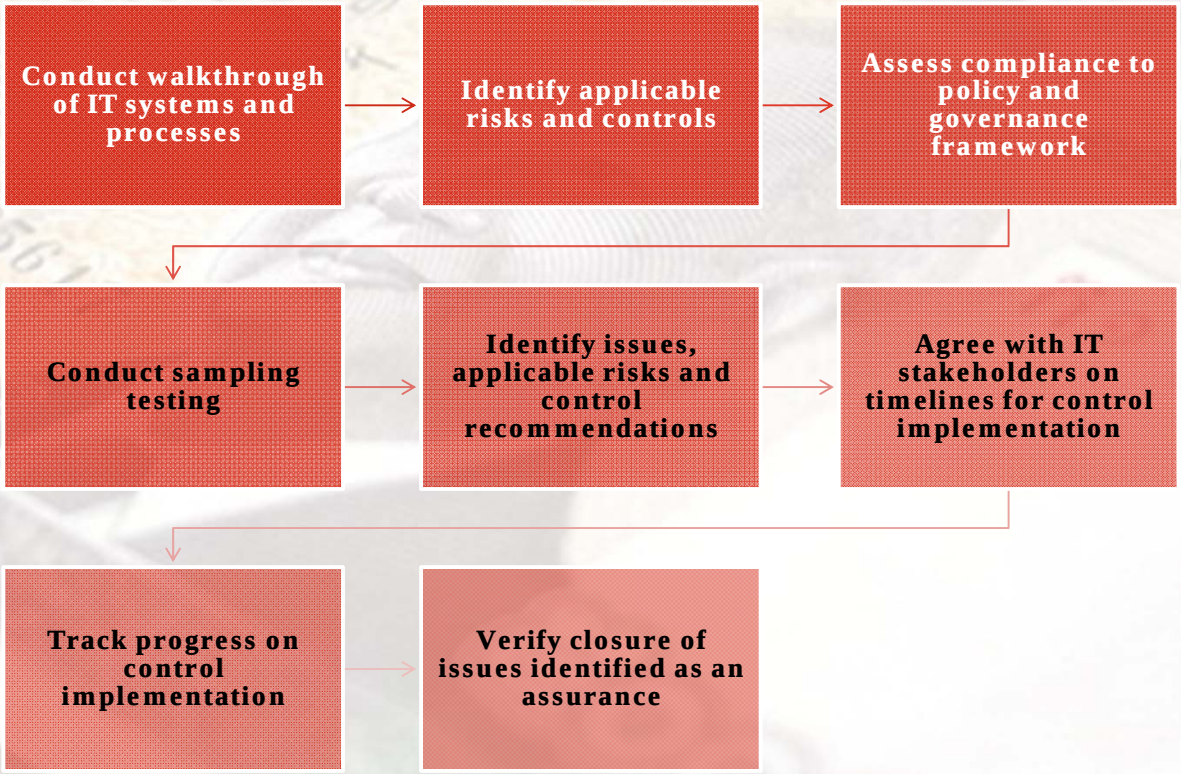
Key takeaways

- Identify the audit landscape around Applications, Applicable Processes, Infrastructure, Teams Responsible while planning an audit
- Inform the Audit Committee of the effectiveness of Risk Management practices and internal control systems
- Define roles and responsibilities along with the time effort required for executing the audit
- In case of specialized audits, understand and agree on the scope based on the risks and threat vectors to be covered
- Consider usage of tools and technologies for effective audit outcomes

5.3. Executing an IS Audit

Key takeaways

- IS auditors to be trained on performing independent audit assurance
- Any issues identified needs to the tracked using a systematic audit remediation or compliance tracking methodology
- Consider information security vulnerabilities applicable to IT systems prior to assessing effectiveness of IT Security risk management framework
- Perform root cause analysis and recommend control implementations for each issue
- Ensure assessment of critical internet based applications is conducted yearly

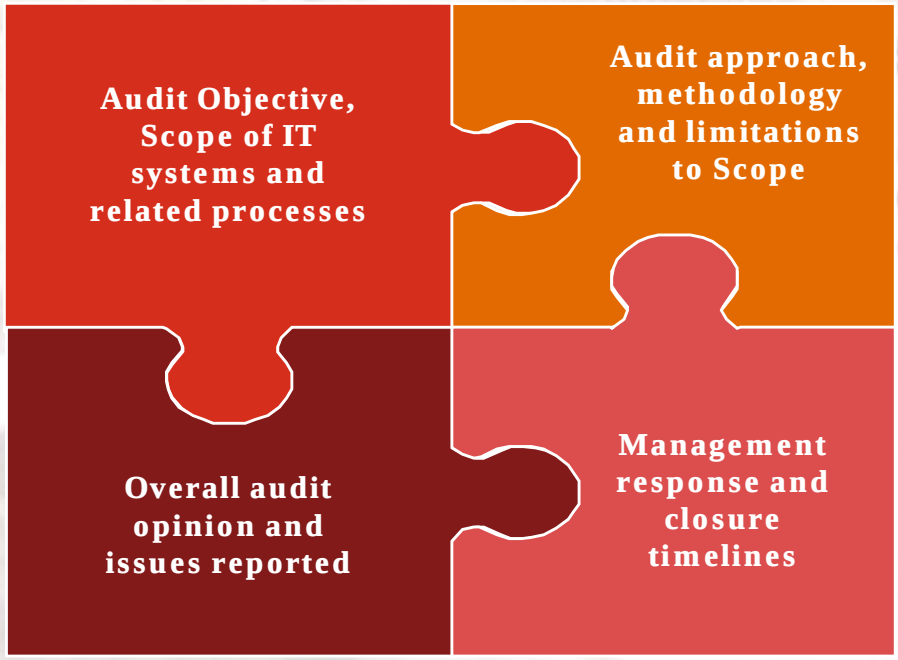


5.4. Reporting and Follow Up

Key takeaways

- Ensure that the audit findings are discussed for accuracy with the IT stakeholders
- A formal response for the non-compliance along with timelines needs to be documented against each issue identified
- IS auditors need to provide an update from planning to audit findings to the Audit Committee
- An audit summary capturing the opinion on control environment posture needs be circulated to all stakeholders involved as part of the audit

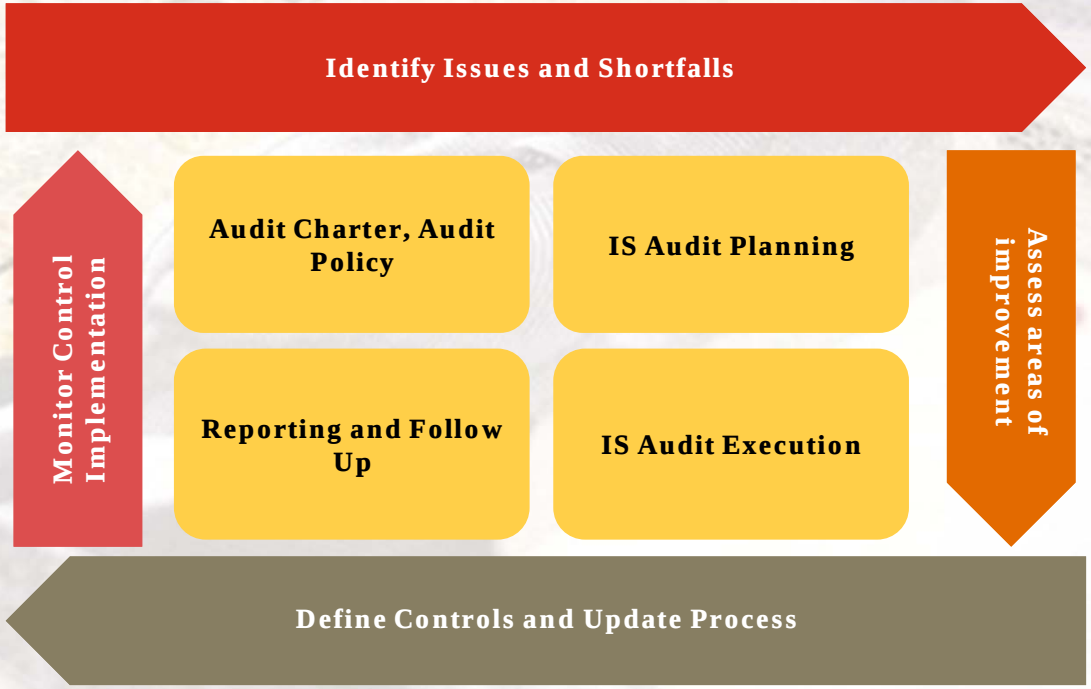
Structure of audit reporting (Illustrative)



5.5. Quality Review

Key takeaways

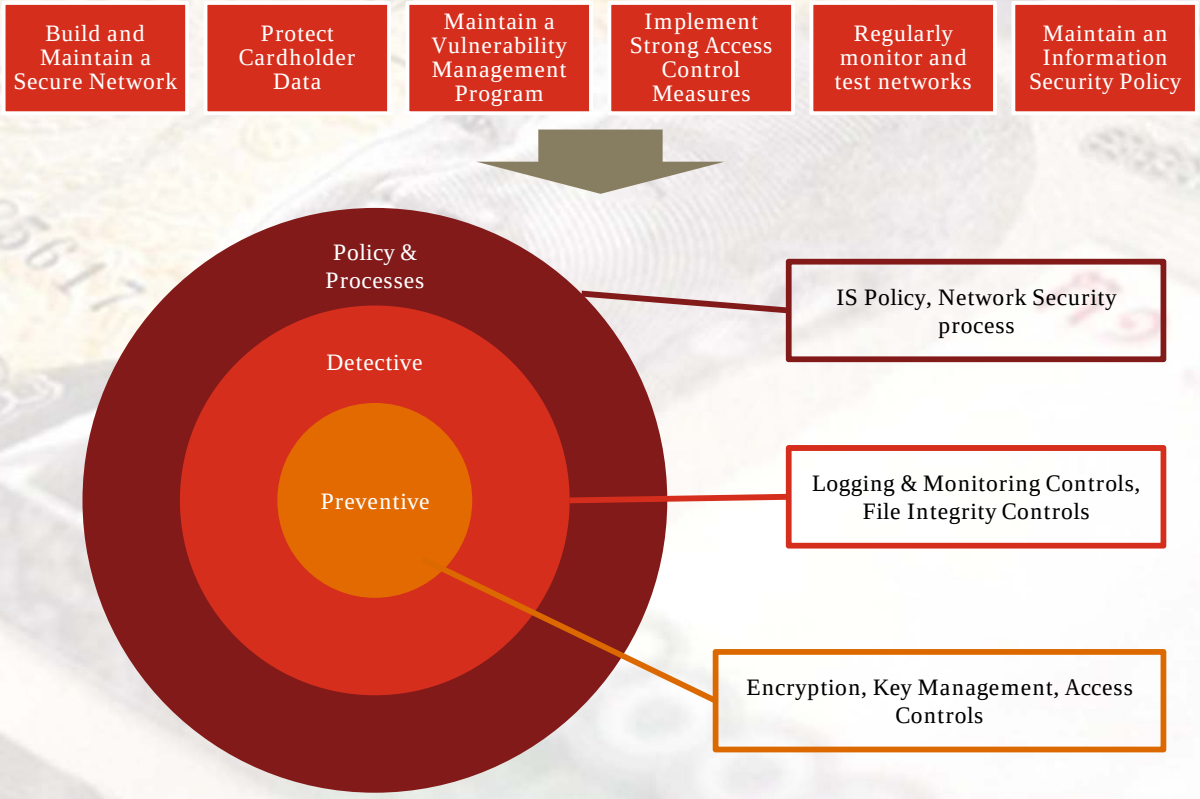
- Identify the shortcomings identified under the following areas as part of the audits performed within organization
    - IS Audit Standards, guidelines, tools and techniques
    - Audit methodology, sampling methodology
    - Planning and project management
    - Evidence collection and retention
    - Audit assurance and reporting to committee
- Assess the shortcomings and identify controls and process to increase efficiency, control and improve quality of the IS Audit



6. Payment Card Security

What is required ?

- Ensure that sensitive payment card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission
- Implement strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (CDA) methods for online and offline card transactions
- Authentication of customers' sensitive static information, such as PINs or passwords shall be performed by the BFIs and not its third party payment processing service provider
- Perform regular security reviews of the infrastructure and processes being used by its service providers



6.1 Protecting cardholder data with security standards

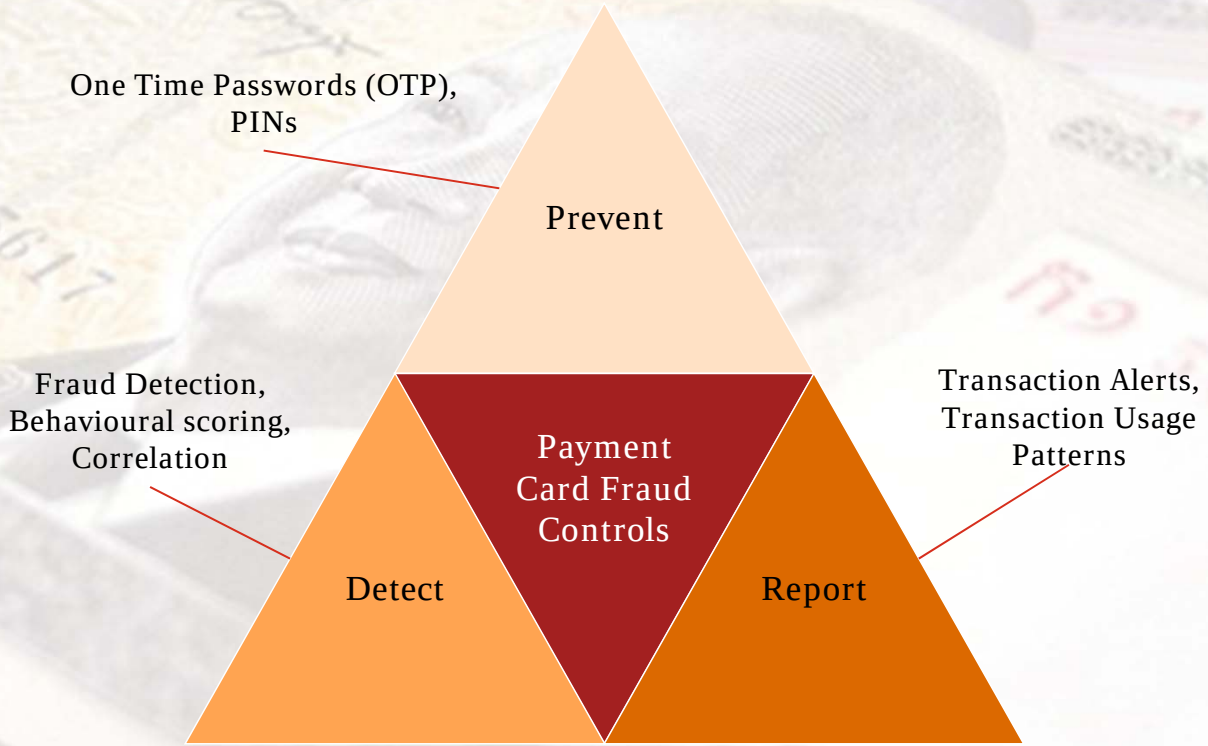
Key takeaways

- Identify cardholder data, taking an inventory of your IT assets and business processes for payment card processing,
- Analyze them for vulnerabilities that could expose cardholder data.
- Remediate vulnerabilities and not storing cardholder data unless you need it
- Report remediation validation records (if applicable) and submit compliance reports to the acquiring BFI and card brands you do business with

6.2 Payment Card Frauds

Key takeaways

- Ensure security controls are implemented at payment card systems and networks
- Implement a dynamic one-time-password (OTP) for CNP transactions via internet to reduce fraud risk associated with CNP.
- Notify cardholders via transaction alerts when withdrawals/charges exceeding customer-defined thresholds made on the customer's payment cards
- Implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities
- Follow up and on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns



Contact us

National Bank of Cambodia
Email: trmg@nbc.org.kh
Tel.: 016 600 700/092 582 187