INFORMATION SECURITY MANAGEMENT

ITIL Lifecycle Poster – Service Design - Process Summary

NISSEN-ITSM

PURPOSE

To align IT security with business security and ensure that the confidentiality, integrity and availability of the organization's assets, information, data and IT services always matches the agreed needs of the business.

TRIGGERS

- New or changed
  - corporate governance guidelines
  - business security policy
  - corporate risk management processes and guidelines
  - business needs or new or changed services
  - requirements within agreements, such as SLRs, SLAs, OLAs or contracts
  - Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Service or component security breaches or warnings, events and alerts
- Periodic activities, such as reviewing, revising or reporting, including review and revision of information security management policies, reports and plans
- Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component

  Requests from other areas, particularly SLM for assistance with security issues.

KEY TERMS

- Availability - Information is available and usable when required
- Confidentiality - Information is observed by or disclosed to only those who have a right to know
- Integrity - Information is complete, accurate and protected against unauthorized modification

INPUTS

- Business information From the organization's business strategy, plans and financial plans, and information on its current and future requirements
- Governance and security From corporate governance and business security policies and guidelines, security plans, risk assessment and responses
- IT information From the IT strategy and plans and current budgets
- Service information From the SLM process
- Risk assessment processes and reports
- Details of all security events and breaches
- Change information
- CMS
- Details of partner and supplier access

Information Security Management

- Produce, maintain ISP
- Communicate, implement, enforce ISP
- Assess, classify information assets and documents
- Implement, review, revise, improve security controls and risk management
- Reviews, audits and penetration tests
- Monitor, analyse, report, reduce and manage security breaches and incidents

ISMS

- Information Security Policy
- Security reports & information
- Security controls
- Security risks & responces

OUTPUTS

- Overall information security management policy, together with a set of specific security policies
- A security management information system (SMIS)
- Revised security risk assessment processes and reports
- A set of security controls, together with details of the operation and maintenance and their associated risks
- Security audits and audit reports
- Security test schedules and plans
- Set of security classifications and a set of classified information assets
- Reviews and reports of security breaches and major incidents
- Policies, processes and procedures for managing partners and suppliers and their access to services and information.