Data Security

1 Introduction

Effective data security policies and procedures ensure the right people can use and update data the right way, and all inappropriate access and update is restricted (Ray, 2012).

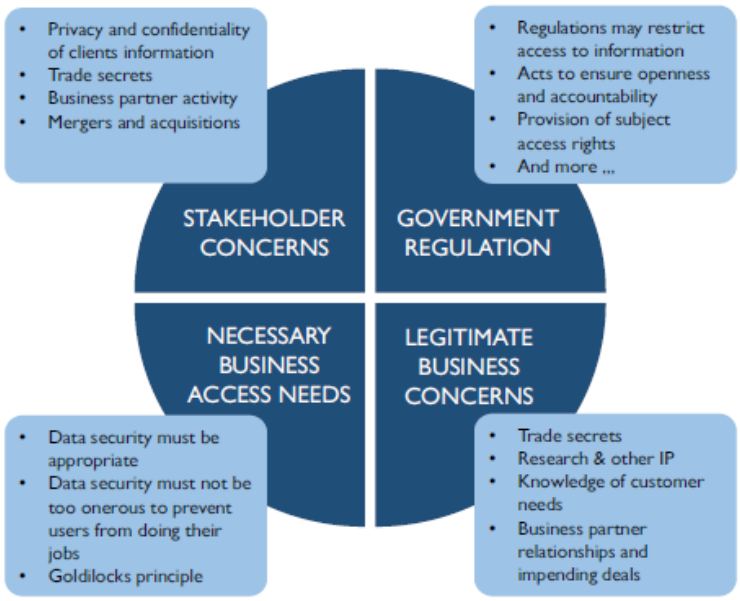
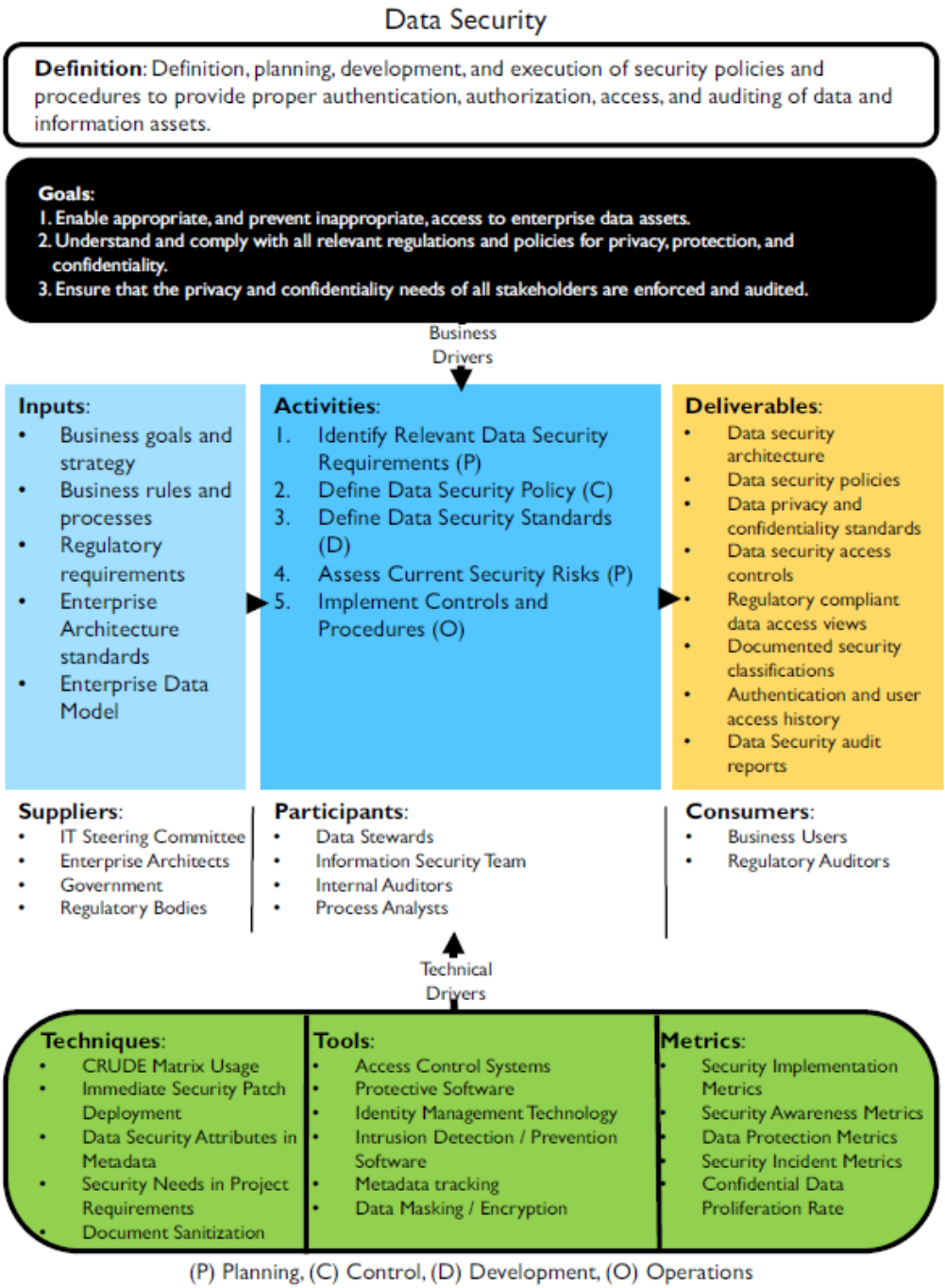


Figure 62 Sources of Data Security Requirements

- **Stakeholders:** Everyone in an organisation must be a responsible trustee of stakeholders' data
- **Government regulations:** Some restrict access and others ensure openness, transparency and accountability
- **Proprietary business concerns:** Data which provides competitive advantage must be protected.
- **Legitimate access needs:**
- **Contractual obligations:** Contractual and non-disclosure agreements



1.1 Business Drivers

Data security risks are associated with regulatory compliance, fiduciary responsibility, reputation and a legal and moral responsibility to protect private and sensitive data. Mitigating risks and growing the business can be complimentary when integrated into an information protection strategy.

- **Risk reduction:** Should be enterprise wide. Classify organisation's data:
  - Identify and classify sensitive data assets
  - Locate sensitive data throughout the enterprise
  - Determine how each asset needs to be protected
  - Identify how the information interacts with business processes
  - Identify external (hackers) and internal (employees and processes) threats.

- **Business Growth:** Data security breaches can impact business growth. Robust data security inspires consumer confidence. Trusted e-commerce drives profit and growth.
- **Security as an asset:** Tag data with security metadata

1.2 Goals and Principles

Goals:

- Enabling appropriate access and preventing inappropriate access to enterprise data assets
- Enabling compliance with regulations and policies for privacy, protection and confidentiality
- Enabling that stakeholder requirements for privacy and confidentiality are met.

Principles:

- **Collaboration**: Data Security is a collaborative effort involving IT security administrators, data stewards/data governance, internal and external audit teams, and the legal department.
- **Enterprise approach**: Data Security standards and policies must be applied consistently across the entire organization.
- **Proactive management**: Success in data security management depends on being proactive and dynamic, engaging all stakeholders, managing change, and overcoming organizational or cultural bottlenecks such as traditional separation of responsibilities between information security, information technology, data administration, and business stakeholders.
- **Clear accountability**: Roles and responsibilities must be clearly defined, including the 'chain of custody' for data across organizations and roles.
- **Metadata-driven**: Security classification for data elements is an essential part of data definitions.
- **Reduce risk by reducing exposure**: Minimize sensitive/confidential data proliferation, especially to non-production environments.

1.3 Essential Concepts

1.3.1 Vulnerability

A **vulnerability** is a weaknesses or defect in a system that allows it to be successfully attacked and compromised – essentially a hole in an organization's defences. Some vulnerabilities are called exploits.

1.3.2 Threat

A **threat** is a potential offensive action that could be taken against an organization. Threats can be internal or external. They are not always malicious. A uninformed insider can take offensive actions again the organization without even knowing it.

1.3.3 Risk

The term **risk** refers both to the possibility of loss and to the thing or condition that poses the potential loss. Risk calculations:

- Probability that the threat will occur and its likely frequency
- The type and amount of damage created each occurrence might cause, including damage to reputation
- The effect damage will have on revenue or business operations
- The cost to fix the damage after an occurrence
- The cost to prevent the threat, including by remediation of vulnerabilities

- The goal or intent of the probable attacker

1.3.4 Risk classifications:

Describe the sensitivity of the data and the likelihood it may be sought after for malicious purposes.

- **Critical Risk Data (CRD)**: Personal information aggressively sought for unauthorized use by both internal and external parties due to its high direct financial value. Compromise of CRD would not only harm individuals, but would result in financial harm to the company from significant penalties, costs to retain customers and employees, as well as harm to brand and reputation.
- **High Risk Data (HRD)**: HRD is actively sought for unauthorized use due to its potential direct financial value. HRD provides the company with a competitive edge. If compromised, it could expose the company to financial harm through loss of opportunity. Loss of HRD can cause mistrust leading to the loss of business and may result in legal exposure, regulatory fines and penalties, as well as damage to brand and reputation.
- **Moderate Risk Data (MRD)**: Company information that has little tangible value to unauthorized parties; however, the unauthorized use of this non-public information would likely have a negative effect on the company.

1.3.5 Data Security Organisation

The Information Security Function depends on the size of the enterprise. May be:

- Dedicated Information Security group within IT
- Chief Information Security officer (CISO) reporting to the CIO or CEO
- Smaller organisations data security is the responsibility of data managers

Dedicated Information Security personnel are most concerned with the technical aspects, such as combating malicious software attacks. Data Management are concerned with regulatory aspects. A standard sharing process should be in place where both groups are kept informed of data regulations, data loss threats and data protection requirements.

NIST (National Institute of Standards and Technology) Risk Management Framework:

- All enterprise information must be categorised.
- The location of all sensitive information must be known.
- Enterprise data model is essential

Data managers, IT Developers and cyber security professionals work together to:

- identify regulated data so that
- sensitive systems are protected
- User access controls designed to
- Enforce confidentiality, integrity and data regulatory compliance

1.3.6 Security Processes

the Four As and an E

- **Access**: Enable individuals with authorization to access systems in a timely manner.
- **Audit**: Review security actions and user activity to ensure compliance with regulations and conformance with company policy and standards.
- **Authentication**: Validate users' access.

- **Authorization**: Grant individuals privileges to access specific views of data, appropriate to their roles.
- **Entitlement**: An Entitlement is the sum-total of all the data elements that are exposed to a user by a single access authorization decision

Systems should include monitoring controls that detect unexpected events. Real time active monitoring for confidential information. System interruption if an event that does not follow procedure occurs. Passive monitoring takes snapshots at regular intervals.

1.3.7 Data Integrity

In security, data security is the state of being whole, protected from improper deletion, alteration or addition.

1.3.8 Encryption

The process of translating plain text into complex codes to hide privileged information, verify complete transmission or verify the sender's identity. Cannot be read without the decryption key. Four main methods of encryption:

- **Hash:** Uses algorithms
- **Symmetric**
- **Private-key:** Both sender and receiver have the same key.
- **Public-key:** Sender uses a public key that is freely available and receiver uses a private key

1.3.9 Obfuscation or masking

The appearance of the data is changed. two types of data masking, Persistent and Dynamic:

- **Persistent data masking:** Permanently and irreversibly alters the data. Used for test environments
    - **In-flight persistent masking:** Data is masked when it is moving from source (production) to destination (non-production). Secure as there is no intermediate file
    - **In-place persistent masking:** Source and destination are the same**.** Unmasked data is read, masked then written over the unmasked data
- **Dynamic data masking:** Makes changes to appearance of data to the end user system without changing the underlying data
- **Masking methods:**
    - **Substitution**: Replace characters or whole values with those in a lookup or as a standard pattern. For example, first names can be replaced with random values from a list.
    - **Shuffling**: Swap data elements of the same type within a record, or swap data elements of one attribute between rows. For example, mixing vendor names among supplier invoices such that the original supplier is replaced with a different valid supplier on an invoice.
    - **Temporal variance**: Move dates +/– a number of days – small enough to preserve trends, but significant enough to render them non-identifiable.
    - **Value variance**: Apply a random factor +/– a percent, again small enough to preserve trends, but significant enough to be non-identifiable.
    - **Nulling or deleting**: Remove data that should not be present in a test system.
    - **Randomization**: Replace part or all of data elements with either random characters or a series of a single character.

- **Encryption**: Convert a recognizably meaningful character stream to an unrecognizable character stream by means of a cipher code. An extreme version of obfuscation in-place.
- **Expression masking**: Change all values to the result of an expression. For example, a simple expression would just hard code all values in a large free form database field (that could potentially contain confidential data) to be 'This is a comment field'.
- **Key masking**: Designate that the result of the masking algorithm/process must be unique and repeatable because it is being used mask a database key field (or similar). This type of masking is extremely important for testing to maintain integrity around the organization.

1.3.10 Network Security Terms: Data-in-motion

- **Backdoor:** A hidden entry to a computer system bypassing password requirements. Usually left by developers for maintenance.
- **Bot or Zombie:** A workstation taken over by a Trojan, Virus, Phish or download of an infected file. Bots are remotely controlled to perform malicious tasks.
- **Cookie:** Small data file an internet commerce website installs on a computer's hard drive to identify returning visitors and their preferences. Could be used by spyware.
- **Firewall**: Software and/or hardware that filters network traffic to protect against unauthorised access or attack.
- **Perimeter**: Boundary between organisation's systems and outside. Firewall sits here.
- **DMZ**: De-militarised Zone. Located between the perimeter firewall and a firewall between it and the internet. Used to pass and temporarily store information moving between organisations
- **Super User Account**: Administrator access to be used in an emergency. Credentials are highly secured and controlled by time, location and user ID.
- **Key Logger**: Attack software that captures keystrokes
- **Penetration testing**: An ethical hacker tries to expose vulnerabilities.
- **Virtual Private Network (VPN)**: Use the unsecured internet to create an encrypted tunnel

1.3.11 Types of Data Security

Data security involves not just preventing inappropriate access, but also enabling appropriate access to data. Access to sensitive data is controlled by granting permissions (opt-in).

- **Facility Security:** Locked data centre
- **Device Security:** Standards for portable devices
  - Access policies regarding connection using mobile devices
  - Storage of data on portable devices
  - Data wiping and disposal of devices in compliance with records management processes
  - Installation of anti-malware and encryption software
  - Awareness of security vulnerabilities
- **Credential Security:** Each user is assigned User ID and Password to access system
  - **Identity management Systems:** Single sign-on gets user onto many systems
  - **User ID Standards for email systems:** Unique within the system. Usually use the user's name in some way.
  - **Password standards:** First line of defence. Should be "strong" and changed every 45-180 days.

    - **Multiple Factor Identification:** Additional identification – code to phone, hardware, biometric.
- **Electronic Communication Security:** Train users not to send confidential information over email or other insecure applications

1.3.12 Types of Data Security Restrictions

Security restrictions are driven by Confidentiality and Regulation:

- **Confidential Data**: Confidential means secret or private and is shared on a "need-to-know" basis. Internally defined. Confidentiality level of a data set depends on the most sensitive item. Typical classification schema:
    - **For General Audiences**: available to anyone
    - **Internal use only**: employees or members. May be discussed but not copied outside the organisation
    - **Confidential**: cannot be shared outside the organisation without a non-disclosure agreement
    - **Restricted Confidential**: Need-to-know
    - **Registered Confidential**: Legal agreement to assume responsibility for the data's secrecy must be signed.
- **Regulated Data:** Regulatory categories are assigned according to laws. Shared on an "allowed-to-know' basis. Externally defined. A single data set may have multiple regulatory categories. It is a good idea to collect many nations personal data privacy laws into a single standard to enforce, achieving international compliance. Sample regulatory families:
    - **Personal Identification Information (PII):** Personally Private Information (PPI). Any information that can identify an individual. EU Privacy Directives
    - **Financially Sensitive Data:** In the US covered by Insider Trading Laws
    - **Medically Sensitive Data / Personal Health Information (PHI):** US covered by HIPAA (Health Information Portability and Accountability Act)
    - **Educational Records:** US covered by FERPA (Family Educational Rights and Privacy Act)
- **Industry or Contract-based Regulations**:
    - **Payment Card Industry Data Security Standard (PCI-DSS):** Any information that can identify an individual with an account at a financial institution.
    - **Competitive advantage or trade secrets**: Protected by industry regulations / Intellectual property laws
    - **Contractual restrictions**: An organisation may restrict how information may be shared in their contracts with others.

1.3.13 System Security Risks

Identify risks inherent in systems:

- **Abuse of excessive privilege:** Principle of least privilege should be applied. Query-level access control is better, but time consuming to set up.
- **Abuse of legitimate privilege:** For unauthorised purposes. Enforce policies for end-point machines using time of day, location and amount of data downloadable.
- **Unauthorised Privilege Elevation:** Convert from ordinary user to Administrator using software vulnerabilities. Prevent with Intrusion Prevention Systems (IPS) and query-level access control.
- **Service account or shared account abuse:**

    - **Service Accounts**: Batch IDs. Untraceable to a particular user.
    - **Shared Accounts:** Generic IDs with one password. Provide ungoverned access.
- **Platform intrusion attacks:** Protect databases with Intrusion Protection and Intrusion Detection Systems. Any update patches should be installed immediately.
- **SQL Injection vulnerability:** A SQL command is inserted in a web input space**.** Sanitise all inputs before passing to server.
- **Default passwords:** Usually supplied by software vendor. Eliminate them
- **Backup data abuse**: Encrypt all database backups and securely manage decryption keys

1.3.14 Hacking/Hacker

A hacker finds unknown pathways in complex computer systems. Can be good or bad:

- White Hat hacker (Western movies the hero always wore a white hat) finds vulnerabilities which are fixed in the patches.
- Malicious hackers intentionally breach systems to steal information or do damage.

1.3.15 Social Threats to Security / Phishing

Involves direct communication to trick people to provide confidential information - Social engineering. Phishing is the call or message.

1.3.16 Malware

Any malicious software created to damage, change or improperly access a computer or network.

- **Adware**: Spyware that slips into the computer from an internet download. It monitors browsing and buying habits. Not illegal.
- **Spyware**: Any program that slips in without consent
- **Trojan Horse**: A malicious program that enters the system embedded in legitimate software.
- **Virus:** A program that attaches itself to an executable file, and delivers a destructive payload
- **Worm**: A program built to reproduce and spread across a network by itself. Usually harms networks by consuming bandwidth.
- **Malware Sources:**
    - Instant Messaging (IM):
    - Social Networking Sites:
    - Spam

2 Activities

2.1 Identify Data Security Requirements

There is no one prescribed way to implement data security. Organisations should design their own security controls.

- **Business Requirements:** Analyse business rules and processes to identify security touch points.
- **Regulatory requirements:** Create a central inventory of all data regulations and the data subject areas affected by each regulation.

Table 13 Sample Regulation Inventory Table

Regulation	Subject Area Affected	Security Policy Links	Controls Implemented

2.2 Define Data Security Policy

Data security policies describe behaviours determined to be in the best interests of the organisation protecting its data. Must be auditable and audited. Requires collaboration between IT Security administrators, Security Architects, Data Governance committees, Data Stewards, internal and external audit teams and the legal department.

Security Policy contents:

- **Enterprise Security Policy:** Global policies
- **IT Security Policy:** Directory structures standards, password policies and identity management framework
- **Data Security Policy:** Categories for individual applications, database roles, user groups and information sensitivity

2.3 Define Data Security Standards

Standards supplement policies and provide detail on how to meet the intention of the policies.

- **Define Confidentiality Levels:** Confidentiality classification is important metadata, guides how users are granted access privileges
- **Define Regulatory Categories:** Regulated Information. Regulations Imply a goal - compliance
- **Define Security Roles:** Two ways to organise
  - **Role Assessment grid:** starting from the data

Table 14 Role Assignment Grid Example

	Confidentiality Level		
	General Audience	Client Confidential	Restricted Confidential
Not Regulated	Public User Role	Client Manager Role	Restricted Access Role
PII	Marketing Role	Client Marketing Role	HR Role
PCI	Financial Role	Client Financial Role	Restricted Financial Role

  - **Role Assessment Hierarchy:** Starting from the User

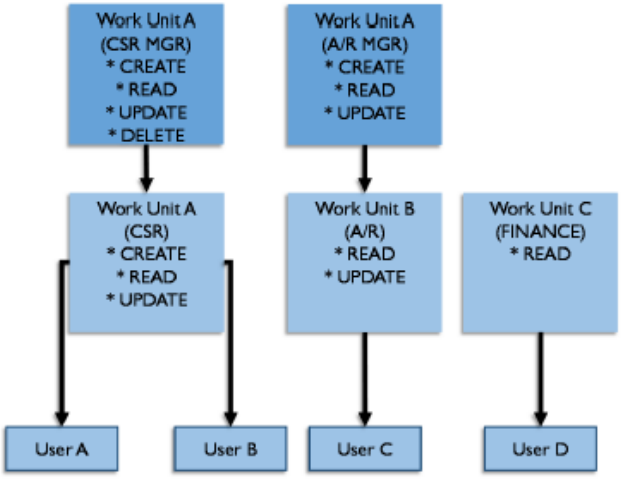


Figure 65 Security Role Hierarchy Example Diagram

- **Assess Current Security Risks:** Identify where sensitive data is stored. Evaluate each system for the following:
  - The sensitivity of data stored of in transit
  - The requirements to protect that data
  - The current security protections in place

  Document the findings as they provide a baseline and may be a requirement of compliance.

- **Implement Controls and Procedures:** Responsibility of security administrators in coordination with data stewards and technical teams. Controls and procedures should at minimum cover:
  - How users gain and lose access to systems
  - How users are assigned to and removed from roles
  - How privilege levels are monitored
  - How requests for access changes are handled and monitored
  - How data is classified according to confidentiality and regulations
  - How data breaches are handled
- **Assign confidentiality levels:**
- **Assign regulatory Categories:**
- **Manage and maintain data security**:
  - Control Data Availability / Data-centric Security
  - Monitor User Authentication and Access Behaviour:
    - Required for compliance audits
    - Lack of automated recording of sensitive and unusual data base transactions represents serious risks
    - Implement a network based audit appliance to mitigate the risks.
- **Manage security policy compliance**
  - Manage regulatory compliance
  - Audit data security and compliance activities

3 Tools

- **Anti-Virus Software / Security Software**
- **HTTPS:** The web address begins https:// a security layer is present

- **Identity Management Technology:**
- **Intrusion Detection (IDS) and Prevention Software (IPS):**
- **Firewalls (Prevention):**
- **Metadata tracking:**
- **Data Masking/Encryption**

4 Techniques

- **CRUD Matrix usage:** Create and use data-to-process and data-to-role relationships
- **Immediate Security Patch Deployment:** No one should be able to delay this update
- **Data Security Attributes in Metadata:** Metadata repository is essential
- **Metrics:** Frame as positive value percentages
    - **Security implementation Metrics:** maintain a reasonable number of actionable metrics in appropriate categories over time to assure compliance
    - **Security Awareness metrics:**
        - Risk assessment findings
        - Risk events and profiles
        - Formal feedback surveys and interviews
        - Incident post-mortems, lessons learned and victim interviews
        - Patching effectiveness audits
    - **Data Protection Metrics:**
        - Criticality ranking
        - Annualised loss expectancy
        - Risk of specific data losses
        - Risk mapping of data to specific business processes
        - Threat assessments
        - Vulnerability assessments
    - **Security Incident Metrics:**
        - Intrusion attempts detected and prevented
        - Return on investment for security costs using savings from prevented intrusions
    - **Confidential Data Proliferation**:
- **Security Needs in Project Requirements:** Identify in the analysis phase
- **Efficient Search for Encrypted Data:**
- **Document Sanitisation:** Clean the Metadata preventing embedded confidential data being shared

5 Implementation Guidelines

- **Readiness Assessment / Risk Assessment:**
    - **Training:** Training on security initiatives at all levels of the organisation
    - **Consistent policies:** Data security policies should align with enterprise policies
    - **Measure the benefits of security:** Link to organisational activities
    - **Set security requirements for vendors:** Include in SLAs and contracts
    - **Build a sense of urgency:** Emphasise legal, regulatory and contractual requirements to build a sense of urgency
    - **Ongoing Communications:**
- **Organisation and Cultural Change:**

- **Visibility into User Data Entitlement:** Requires Metadata of classification and the authorisations themselves
- **Data Security in an Outsourced World:** Anything can be outsourced except liability.
    - Tighter management of control mechanisms
- **Data Security in Cloud Environments:** Data security policies should account for data distributed over these platforms, and should be the same as the rest of the enterprise

6 Data Security Governance – Data Security and Enterprise Architecture

Requires cooperation between IT and business stakeholders, and strong policies and procedures.

Data security Architecture is a component of enterprise architecture that describes how data security is implemented. Architecture influences:

- Tools used to manage data security
- Data encryption standards and mechanisms
- Access guidelines to external vendors and contractors
- Data transmission protocols over the internet
- Documentation requirements
- Remote access standards
- Security breach access reporting

Security architecture is particularly important for integration of data between:

- Internal systems and business units
- an organisation and its external business partners
- An organisation and regulatory agencies