DATA SECURITY

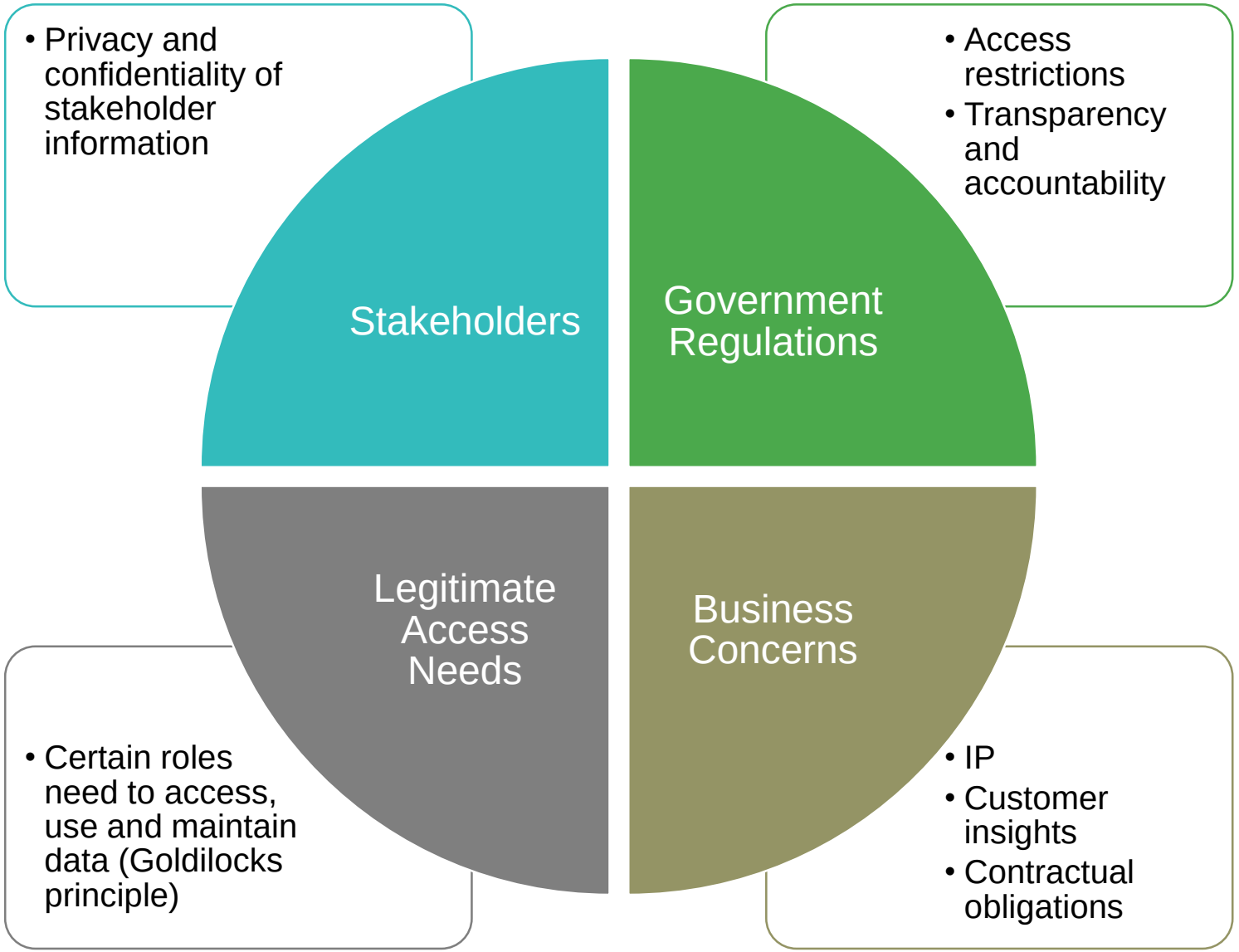
Objectives

- To define Data Security
- To explain Information Risk
- To describe techniques for Data Protection

Agenda

- **What is Data Security**
- What is Information Risk
- Methods of Data Protection

Data Security **is the planning, development and execution of security policies and procedures to provide proper authentication, authorisation, access and auditing of data assets. The goal is to protect data assets in alignment with:**



Adapted: DMBOK2

Data Security

Definition: planning, development and execution of security policies and procedures to provide proper authentication, authorisation, access and auditing of data and information assets

Goals:

- Enable appropriate, and prevent inappropriate, access to data assets
- Enable compliance with external and internal obligations for privacy, protection and confidentiality
- Ensure stakeholder requirements for privacy and confidentiality are met

Principles:

- Collaboration: collaborative effort of all roles
- Enterprise-approach: consistently applied across entire organisation
- Proactive management: engage all stakeholders, manage change and overcome “silos of responsibility”
- Clear accountability: clearly defined roles & responsibilities, including “chain of custody” of data across organisations/roles
- Metadata-driven: security classification an essential part of data definition
- Reduce risk by reducing exposure: minimise sensitive/confidential data proliferation

Business Drivers:

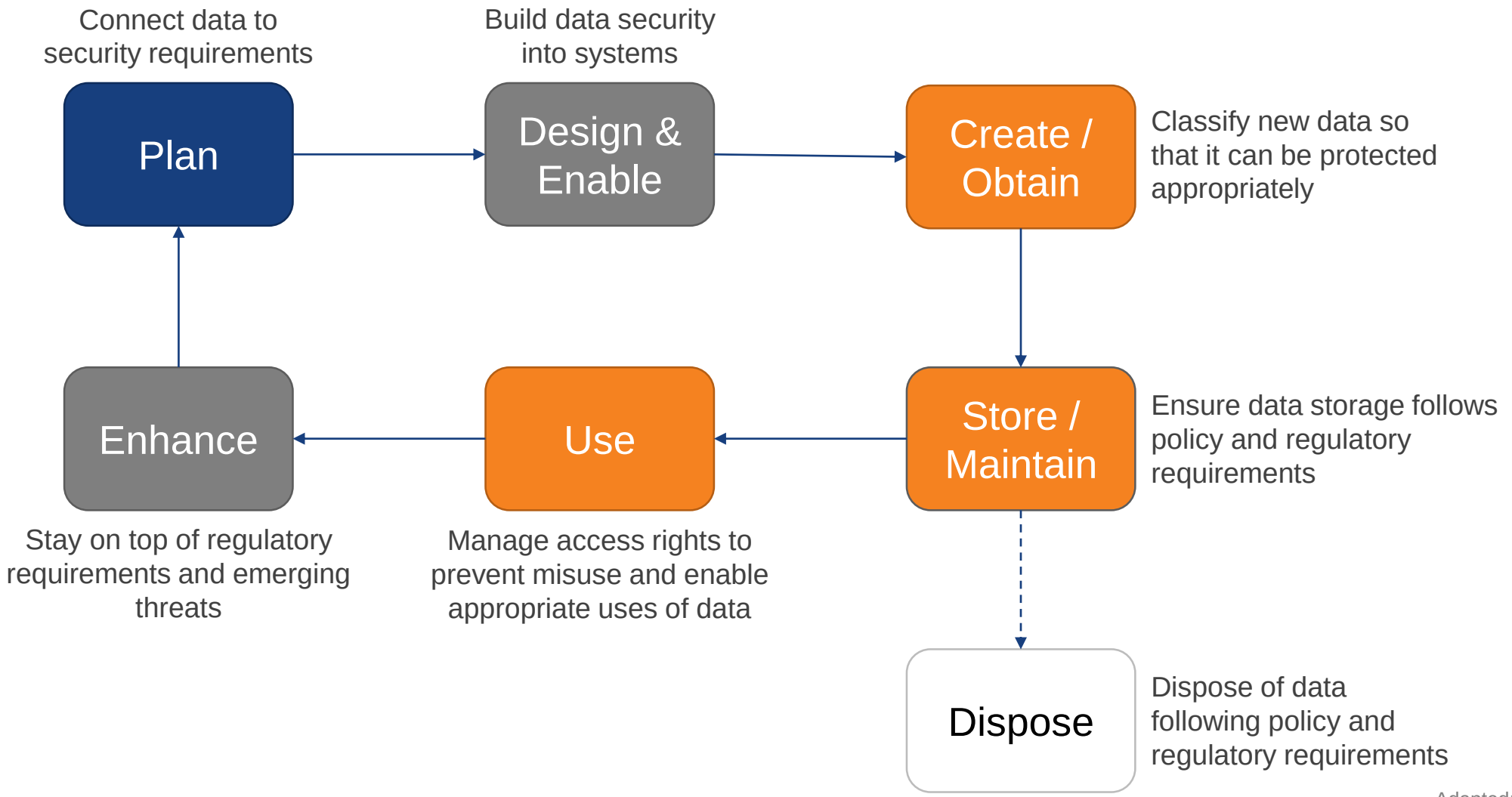
Risk Reduction:

- Reputation
- Compliance
- Fiduciary responsibility
- Ethical

Business Growth:

- Attain and sustain business goals
- Build customer trust

Data Security across Data Lifecycle



Adapted: DMBOK2

Data Security Context

Business Drivers: Risk Reduction / Business Growth

Inputs:
- Business goals and strategy
- Business rules and processes
- Regulatory requirements
- Enterprise Architecture standards
- Enterprise data model

Activities:
- Identify relevant data security requirements
- Define data security policy
- Define data security standards
- Assess current security risks
- Implement controls and procedures

Deliverables:
- Data security architecture
- Data security policies
- Data privacy and confidentiality standards
- Data security access controls
- Regulatory compliant data access views
- Documented security classifications
- Authentication and user access history
- Data security audit reports

Suppliers:
- IT Steering Committee
- Enterprise Architects
- Government
- Regulatory bodies

Participants:
- Data Stewards
- Information Security Team
- Internal Auditors
- Process Analysts

Consumers:
- Business Users
- Regulatory Auditors

Technical Drivers:

Techniques:
- CRUD matrix usage
- Immediate data security patch deployment
- Data security attributes in metadata
- Data security needs in project requirements
- Document sanitisation

Tools:
- Access control systems
- Protective software
- Identify management technology
- Intrusion detection / prevention software
- Metadata tracking
- Data masking / encryption

Metrics:
- Security implementation metrics
- Security awareness metrics
- Data protection metrics
- Security incident metrics
- Confidential data
- Proliferation rate

Agenda

- What is Data Security
- **What is Information Risk**
- Methods of Data Protection

Information Risk

"Information risk management (IRM): The policies, procedures, and technology one adopts in order to reduce the threats, vulnerabilities, and consequences that could arise if data is not protected."

– *BitSight*

Risk

=

Threat x Vulnerability x Consequence

"…is to enable decision makers who are responsible for information and systems to understand key information risks and agree upon the controls required to keep those risks within acceptable limits.

– *SANS Institute*

Risk Equation

- **Risk**
  - Possibility of loss
  - Thing or condition that poses the potential loss
- **Threat**
  - Unintentional – data is mishandled or infrastructure is mismanaged by employees
  - Intentional – hackers, for malice or gain
- **Vulnerability**
  - Gaps in how the information is protected
  - Understanding of how the gaps can be exploited
- **Consequence**
  - Value of information to the organisation
  - Legal requirements for protecting the information

Elements of Control

- **Policies, examples**
  - Acceptable Use Policy
  - Data Management Policy
  - Research Data Management Policy
  - Personal Data Policy
- **Procedures, examples**
  - Data classification
  - Impact assessments, e.g., Data Protection Impact Assessment (DPIA)
  - Data sharing procedures
- **Technology, examples**
  - Multi-factor authentication
  - Anti-virus
  - Firewalls
  - Intrusion detection

Agenda

- What is Data Security
- What is Information Risk
- **Methods of Data Protection**

DATA CLASSIFICATION

Data Classification

Data classification helps organisations

- Discover what data they hold
  - Depending on the industry and organisation, there can be few or many data assets, and a range of sensitive data, e.g., personal identification, medical, financial, etc.
- Where it is located
  - Security requirements may differ, depending on where data is stored. A significant amount of sensitive data in a single location poses a high risk due to the damage possible from a single breach
- What level of protection it should receive
  - The measures necessary to ensure security can vary between data assets depending on data content and the type of technology
- How it interacts with business processes
  - Analysis of business processes is required to determine what access is allowed under what conditions; how long it must be retained; etc.

Data Classification, Example

Data[1] Classification	Organisational Risk from Disclosure	Description	Examples
Confidential	High	Data which are sensitive or critical for use by authorised personnel on a need-to-know basis	• Salary • Appraisal • Personal data • Financial information
Restricted	Moderate	Data other than those classified *Confidential* for use by authorised personnel on a need-to-know basis	• Staff records • Management information • All personal data other than those classified *Confidential*
Internal	Low	Data for use within the organisation	• Staff circulars • Internal policies
Public	None	Data which can be made available or are already available to the public	• Press releases • Newsletters • magazines

[1] *Data includes data elements, information, documents or materials*

Potential Impact

Security Objective	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Source: *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*

Considerations

- Data classifications are used ***enterprise-wide***; classification of data should be performed by an appropriate ***Data Steward***
- A collection of data (single function / purpose) may be assigned a single classification; which should be the most ***restrictive*** of any individual data element
- Re-evaluate classification periodically; any change should also result in associated ***protection control*** being re-evaluated and re-aligned if necessary

Consideration

- **Consider potential impact**
  - Confidentiality – ***security*** of the data to be classified
  - Integrity – low-quality data cannot be ***trusted***
  - Availability – high availability needs ***resilient*** storage and networking
- **Consider costs**
  - It takes ***effort*** to classify and maintain every data element
  - It takes ***even more effort*** to satisfy, maintain and comply with every item of classified data

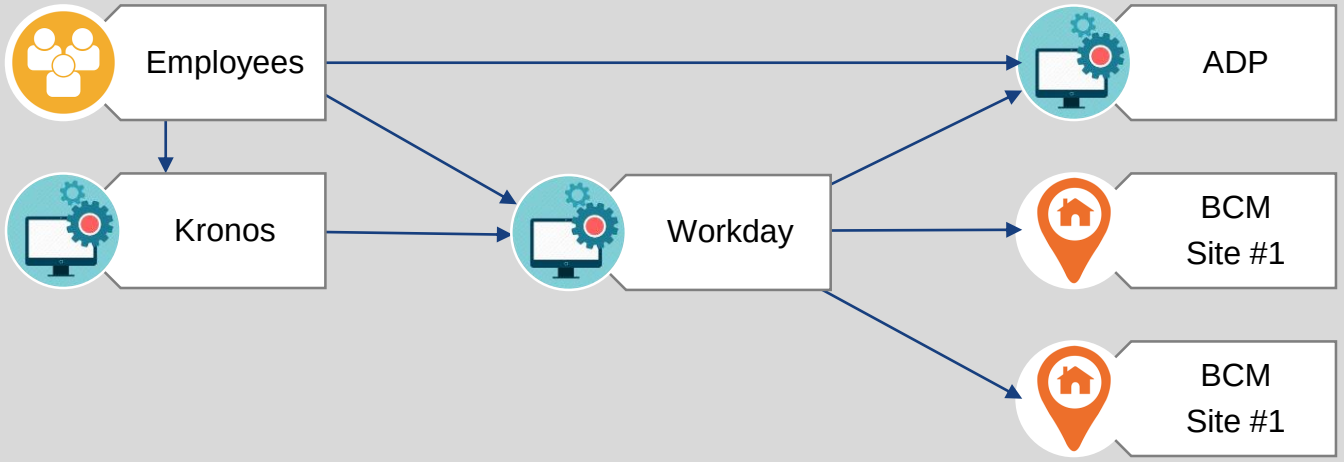
DATA MAP

What is a Map

Geographic Map – Locations & Paths

Data Map – Inventory & Flows

Risk	Process	Data Collected	Data Domain	Sensitive	Data Subjects	Data Locations
High	Payroll Processing	• Name • Personal Identification Number • Salary	• Personal Data • Financial Data	Yes	Employees	• Local • Cross-Boundary
High	Payment Processing	• Name • Personal Identification Number • Credit Information	• Personal Data • Financial Data	Yes	Customers	• Local • Cross-Boundary



Incorporate Existing Inventory

ID	Business Data Object	Field Name	Description	Alternate Names	Associated Business Data Object	Data Field	Unique Values?	Data Type	Length	Valid Values	Default Value
DQ000	Customer	Customer Name	The full name of the customer, including aliases, nicknames and form of address		CustName	customer name	N	Alphanumeric	100	Any	
DD001	Order	Shipping Address	The entire shipping address for the order	Ship-to Address	Address	shipping address	N	Alphanumeric	50	May only contain letters, digits and periods. May not contain a "PO" or "P.O." as a word. Case insensitive	Customer's preferred Shipping Address if returning customer, otherwise null
DD002	Order	Billing Address Same As Shipping	An indicator of whether the shipping address and the billing address are the same		N/A	billing address same	N	Boolean	N/A	True/False	Customer's preferred setting if returning customer, otherwise TRUE
DD003	Order	Billing Address	The entire billing address for the order		Address	billing address	N	Alphanumeric	50	May only contain letters, digits and periods	Customer's preferred Billing Address if returning customer, otherwise null
DD004	Order	Coupon Code	Payment can be made in full or partial with use o valid promotional coupon or codes	Valid system coupon	N/A	payment coupon	N	Alphanumeric	15	Any	null
DD005	Order	Payment Info Subtotal	Subtotal of price of items in cart	Cart subtotal	N/A	payment subtotal	N	Currency	10	0.00…999,999.99	null
DD006	Order	Payment Info Sales Tax	Sales tax added to the order sutotal depending upon customer's location	Sales Tax $	N/A	payment tax	N	Currency	10	0.00…999,999.99	null

Incorporate Existing Inventory

ID	Business Data Object	Field Name	Calculation	Reqd?	Business Rules	Customer Role	Sales Rep Role	Track Changes?	Owner	Status	PII	Notes
DQ000	Customer	Customer Name	N/A	Y	N/A	View, Edit	View, Edit	Yes	Customer Relations Team	Reviewed	Yes	
DD001	Order	Shipping Address	N/A	Y	N/A	View, Edit	View, Edit	Yes	Purchase Team	Reviewed		
DD002	Order	Billing Address Same As Shipping	N/A	N	N/A	View, Edit	View, Edit	Yes	Purchase Team	Reviewed		
DD003	Order	Billing Address	N/A	Y	N/A	View, Edit	View, Edit	Yes	Purchase Team	Reviewed		
DD004	Order	Coupon Code	N/A	N	Must be a legitimate coupon code that is still valid (not expired) and not redeemed	View, Edit	View, Edit	Yes	Business SME	Draft		
DD005	Order	Payment Info Subtotal	If a "Dollar Off" coupon code is entered: Sum of the price of all items in the cart minus the coupon amount. If result is < 0, then 0. If a "Percent Off" coupon code is entered: (Sum of the price of all items in the cart) * (100-Percent Off)/100, rounded to the nearest cent (round 0.5 up). Otherwise: Sum of the price of all itmes in the cart	Y	N/A	View	View, Edit	Yes	Finance	Draft		
DD006	Order	Payment Info Sales Tax	Tax calculated using Payment Info Subtotal and Shipping Address; see "tax calculations"	Y	See "tax calculations"	View	View	Yes	Finance	Draft		

Steps to Data Mapping

To effectively map data, understand the information flow, describe it and identify its elements.

Understand

An information flow is a transfer of information from one location to another. A location can be a:

- System
- Role
- Process
- Location

Describe

- Walk through the information lifecycle to identify unforeseen or unintended uses. This helps minimise what data is collected
- Consider the potential future uses of the information even though it is not immediately necessary

Identify

- Data item; what kind of data is being processed?
- Format; what format is data stored?
- Transfer; how is data collected and how is it transferred between locations?
- Location; where are the locations, e.g., on-premise, cloud, etc.
- Accountability; who is accountable for the data at each location?
- Access; who has access to the data at each location?

Considerations

- What data is collected
- Who are the data stewards
- Who has access within / outside the organisation
- Where is the data logically / physically
- Is there encryption at-rest / in-transit
- Is the data transformed
- Is data retention correctly managed

Key Challenges

- Identifying the data, which can reside in different locations in different formats, such as paper, electronic, video and audio
- Identifying appropriate technical / organisational safeguards
- Understanding internal and external obligations

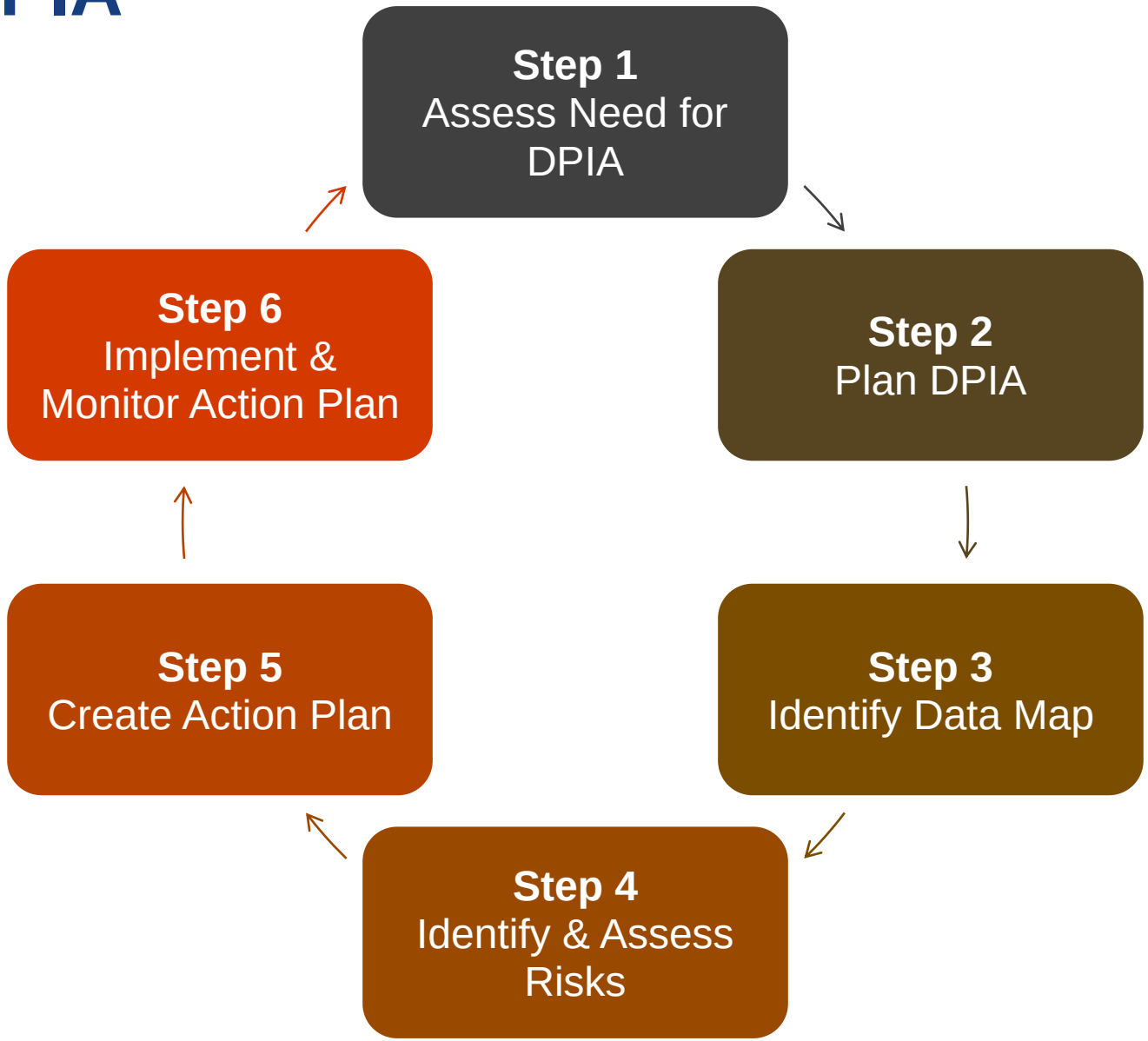
IMPACT ASSESSMENT

Data Protection Impact Assessment

An assessment of how data is handled

- To ensure handling of data *conforms* to applicable legal, regulatory or policy requirements
- To determine *risks and consequences* of collecting, using and disclosing data
- To examine and evaluate the data protection mechanisms in place and to *mitigate* potential risks

Steps to DPIA



① Assess Need for DPIA

Data protection needs to be addressed when:

- A system or process is new and in the process of being designed, *or*
- The system or process is undergoing changes, *or*
- There are changes to compliance requirements

② Plan DPIA

Planning needs to cover the key aspects:

- Describe the objective/background, timeline, why a DPIA is needed, etc.
- Describe the system or process against which the DPIA is to be carried out
- Define the risk assessment framework
- Identify the parties involved and how their views would be sought, e.g., interviews, workshops, consultation, etc.
- Estimate the effort involved and overall timeline

③ Identify Data Map

- **Collate and review all related documentation to determine how data is collected, used, disclosed and retained, e.g.,**
  - Functional / requirement specifications
  - Contracts with external parties
- **As data mapping proceeds, identify gaps for improvement, e.g.,**
  - Security measures
  - Training of staff
  - Agreements with third-parties

④ Identify & Assess Risks

- **Create a data assessment questionnaire based on:**
  - Relevant legislation
  - Sectoral regulations / guidelines
  - Internal policies / procedures
  - Industry good practice
- **Complete the questionnaire based on the Data Map**
- **Analyse impact and likelihood of identified gaps; determine risk based on the pre-defined risk framework**

⑤ Create Action Plan

Propose how the identified risks should be addressed:

- Recommend the specific measures to address each risk
- Identify owners for each set of measures
- Describe the implementation timeline and how the outcomes will be monitored

⑥ Implement & Monitor Action Plan

- **Document the whole DPIA process:**
  - How was it scoped, planned and executed
  - What are the findings
  - What is the proposed action plan
- **The report should be reviewed for compliance with:**
  - Relevant legislation
  - Sectoral regulations/guidelines
  - Internal policies/procedures
  - Industry best practice
- **Upon successful review, the report should be submitted to governance oversight to seek approval to implement the action plan**
- **The action plan must be monitored to:**
  - Successful conclusion, *or*
  - A change necessitating review of the DPIA

Summary

- Information Risk Management is part of the broader organisational Risk Management
- A Data Map is “living” and should be re-assessed periodically
- A DPIA works best when it evolves with its project

THANK YOU

nicholas_tan@nus.edu.sg