
DATA PROTECTION COMMISSION
Building Integrity and Trust
MINISTRY OF COMMUNICATIONS
2017
DATA PROTECTION
CONFERENCE

BREAKOUT SESSION 1

Getting Ready - Data Protection Audit

AGENDA

- Data Protection Audit (DPA): Definition, Why, Benefits & Requestor
- Audit Cycle, Audit Preparation & Tasks
- Audit Categories : Adequacy Audits & Compliance Audits
- Auditors' Objectives
- Audit Document Evidence
- Risk Assessment

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Data Protection Audit : Definition

It is a systematic & independent examination to determine whether…

- personal data processing activities are carried out in accordance with the data protection policies & procedures of the organisation

- data processing meets the requirements of the Data Protection Act, 2012

  (Act 843)

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Data Protection Audit : Definition - Key take outs

- It is a **systematic approach**
- Carried out ideally **by certified independent auditors**
- Conducted in accordance with a **documented audit procedure**
- Outcome is documented in an **Audit Report**

Data Protection Audit: Why?

- To assess the level of compliance with the **Data Protection Act, 2012 (Act 843)**
- To assess the level of compliance with the **organisation's own data protection system**
- To **identify potential gaps** and weaknesses in the data protection system
- To provide information for data protection **system review**

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Data Protection Audit: Benefits

- **Facilitates compliance** with the Data Protection Act
- Measures & **helps improve compliance** with the organisation's data protection system
- Increases level of **data protection awareness** for management & staff
- Provides information for data protection **system review**
- **Improves customer satisfaction** by reducing the likelihood of errors leading to customer complaints

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Data Protection Audit: Requestor

- Request by **Data Controller**
- Decision made by **Data Protection Commission** (The Regulator)
- **Random Audits** conducted by Data Protection Commission

Data Protection Audit goes beyond the

basic requirements of Data Security and

addresses wider aspects of data protection including…

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

- Mechanisms to ensure that information is obtained & processed fairly, lawfully & adequately
- Quality Assurance to ensure that information is accurate, complete, updated & relevant
- Retention of appropriate data, cleaning & deletion of excessive information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines et-c
- Compliance with individuals' rights, such as subject access requests.
- Compliance with data protection legislation in the context of other aspects of legislation such as the Human Rights Act

Data Protection Audit – Cycle

1. **Audit Planning**
2. **Audit Preparation**
3. **Conduct of the Compliance Audit**
4. **Compliance Audit Reporting**
5. **Audit Follow-Up**

Duration – will be advised by Auditors prior to visit

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Data Protection Audit – Preparation

Data Protection Training

- Data Protection Supervisor
- Staff with data protection responsibilities need specific days dedicated to training
- IT Staff

Preparation Tasks

- Data Protection Supervisor
  - Main point of contact
  - Available for Audit duration
    - Auditor may have questions
    - May need to speak to other staff
    - May need information.
- Notify staff: IT System & staff with expertise should be available
- Make desk / office available for auditor

Management Support Essential

Data Protection Audit: 3 main Audit Categories

Description	Audit Category	Conducted By
First Party	Internal	By the Organisation itself
Second Party	Supplier	By the Organisation on a Supplier or Sub-contractor
Third Party	External	By the DPC, its Sub-contractors or an independent certified consultant of the organisation

Data Protection Audit: Overview

External or Supplier Audit

Adequacy Audit

Data Protection Act, 2012 (Act 843)

Data Protection Policy

Compliance Audit

Data Protection Act Procedures, Guidelines, Codes of Practice et-c.

Forms, Files, Records, Databases involving Personal Data

Internal Audit

Compliance Audit

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Adequacy Audits: Purpose & Rating

PURPOSE

Check if documented Policies, Codes of Practice, Guidelines & Procedures meet requirements of Data Protection Act

- a desktop exercise that can usually be conducted off-site.
- can be conducted by Internal Auditors provided they have the requisite understanding of the requirements of the Data Protection Act

RATING

Satisfactory Adequacy Audit
Indication of small number of gaps or deficiencies, the Auditor can continue with a Compliance Audit

Unsatisfactory Adequacy Audit
Indication of very little data protection documentation in place with inadequate procedures and major gaps in areas such as data protection awareness training.

Adequacy Audits: Unsatisfactory Rating next steps

Auditors MUST make a policy decision on how to proceed - **3 Options**:

1. The organisation may still wish to go ahead with a Compliance Audit to help **formulate potential solutions to address the key gaps** and weaknesses already identified in its systems

2. The Auditors **should inform the organisation to fix major deficiencies** before proceeding to Compliance Audit.

3. The Auditors **should refer the organisation to the DPC** or others providing data protection advice and guidance to rectify the deficiencies in the data protection system.

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Compliance Audits: Purpose & Process

PURPOSE

Check that the organisation is operating in accordance with its documented Policies, Codes of Practice, Guidelines and Procedures. Must be conducted on-site.

PROCESS is conducted **Internally** because

- It is more effective to carry out scheduled Internal Audits on data protection system that have been formally documented and are fully operational.
- The data protection system should meet the requirements of the Data Protection Act
- If the data protection system is mature, it should have been subjected to an earlier Adequacy Audit by independent third parties as part of the implementation process.

However, organisations can also conduct Adequacy Audits as part of their Internal Audit programmes which could be beneficial for the implementation of a new system

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

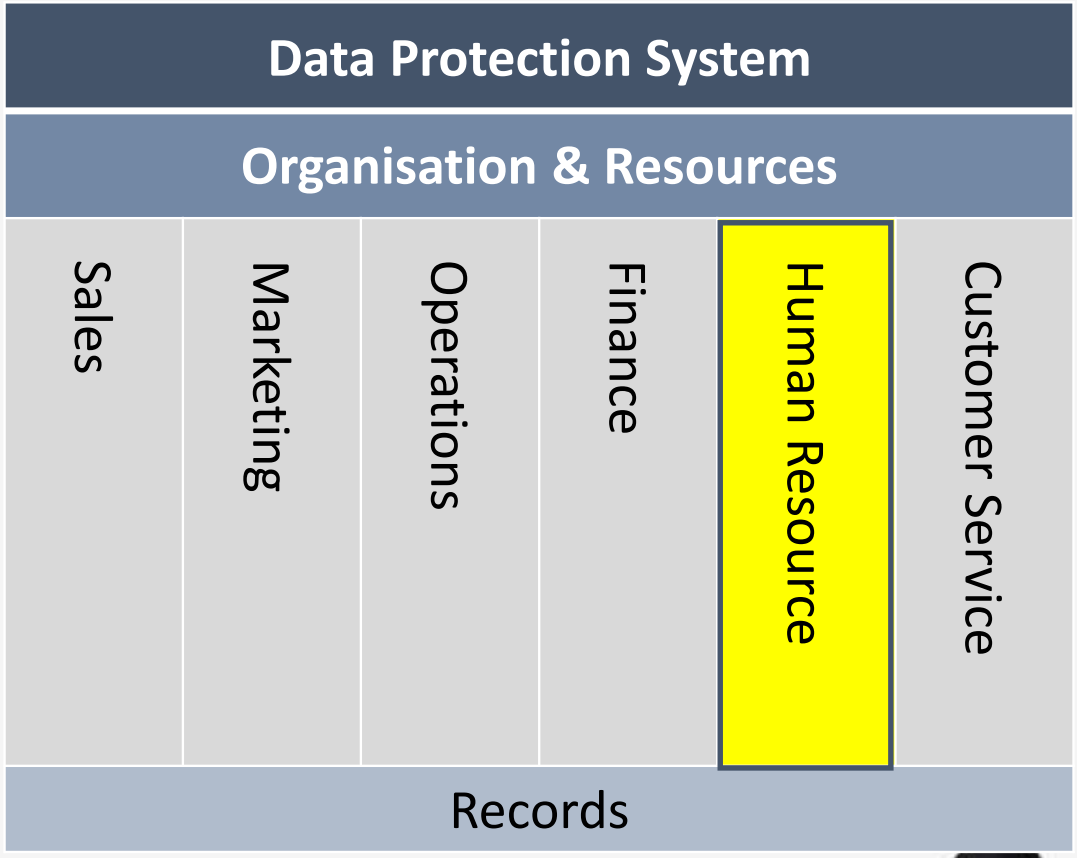
Compliance Audits: Methodologies

2 basic methodologies - used separately or in combination

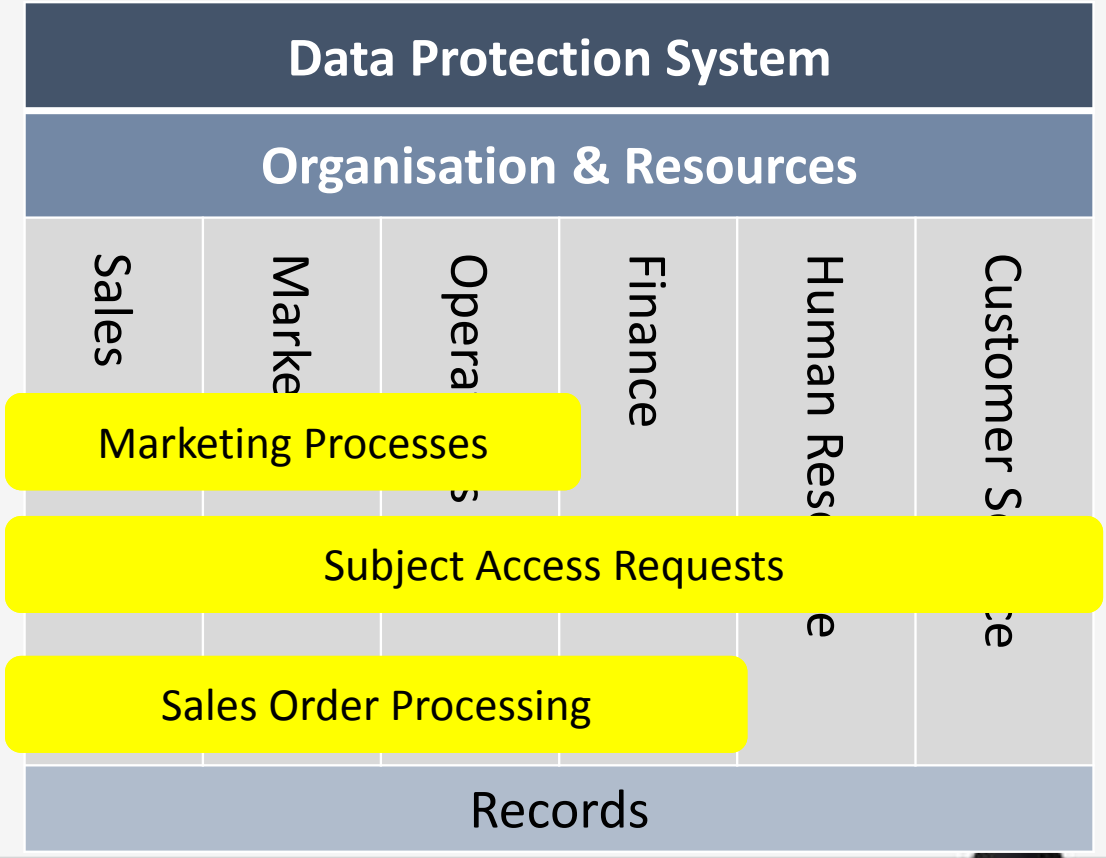
1. Functional or Vertical Audit

2. Process or Horizontal Audit

Compliance Audits: Functional or Vertical



Compliance Audits: Process or Horizontal



Data Protection Audit: Auditors' Objectives

- Verify that there is a formal (i.e. documented & updated) data protection system in place within the organisation

- Verify that all the staff within the organisation involved in data protection…
  - are aware of the existence of the data protection system
  - understand the data protection system
  - use the data protection system

- Verify that the data protection system within the organisation actually works and is effective

Audit Document Evidence

Internal and External Auditors look for documented evidence concerning different aspects of a data protection system.

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Audit Document Evidence

Example

Audit Objective	Documented Evidence Sought	Adequacy Audit	Compliance Audit
The System EXISTS & is ADEQUATE	Documentation example – Data Protection Policy, Procedures et-c	YES	YES
The System is UNDERSTOOD & Correctly USED	Records of Subject Access Request, Complaints et-c	NO	YES
The System WORKS	Corrective Actions, System updates and improvements	NO	YES

Audit Document Evidence

- Registration – Valid and Updated
- Documentation - *content quality is vital*

  exa*mples*
  - **Latest Risk Assessment**: subsequent reviews, policies, good practice guidelines, evidence of training, issue log, code of conduct et-c.
  - **IT Systems**: security updates, licences, data backup and recovery procedures, data breach procedures, disaster recovery, mobile devices et-c.
  - **Data Subject Participation**: data subject request log, data subject's rights et-c.
  - **Data Processor**: confidentiality contracts, evidence of monitoring et-c.

Audit Document Evidence

- Data Protection - embedded
  - The Staff : Level of Awareness
  - The Processes : Is Privacy well Understood
  - The IT Systems: Usage Policy, Access Level Control, Physical Security
- Auditors may request for certain documents prior to visit
  - To be used to decide activity areas for inspection and/ or for particular attention
- Observation of workplace environment
  - Confidential documents left at printer/photocopier
  - Computers left unattended to or unlocked
- Auditors can speak to the staff involved in the activities being audited. This dialogue should occur through
  - Staff Questioning
  - Staff Awareness interviews

Risk Assessment: Rational

To identify **Potential Risks** of personal data & **eliminate / mitigate those risks**

Failure to manage the risks, result in Individual AND Organisational Risks

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Cycle

Risk Assessment: Planning

1. Formulate Questions for Answers to help identify Potential Risks

Some relevant sections
1st Principle: lawful and reasonable processing
2nd Principle: S19 - necessary, relevant, not excessive S20 - prior consent
3rd Principle: specific lawful purpose. Data subject must be aware

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Planning

2. Identify Activities that Process Data

follow the flow of data

Collection → Primary Use → Update / Sharing → Secondary use/reuse → Disposal

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Planning

- Who provides the personal data?
- What specific items of data are collected?
- Why is the data collected?

Collection → Primary Use → Update / Sharing → Secondary use/reuse → Disposal

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Planning

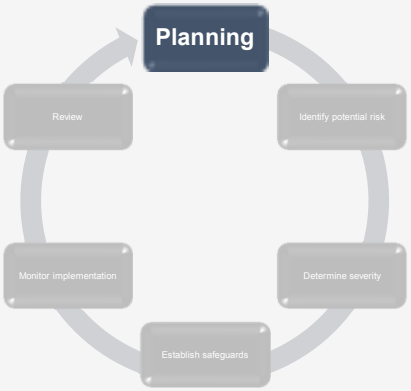
- What activities collect Personal Data?
- Who undertakes each activity?
- Where is the personal data stored for each?

Collection → Primary Use → Update / Sharing → Secondary use/reuse → Disposal

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Planning



- Is the personal data used for anything else?
- If the personal data is used by anyone else *(who? & what purpose?)*
- What happens after this activity & who undertakes the next activity?

Collection → Primary Use → Update / Sharing → **Secondary use/reuse** → Disposal

Secondary use occurs outside primary flow: Check IT systems, Sales, Marketing; Investigate teams not captured in data flow

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

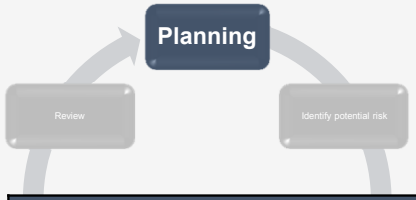
Risk Assessment: Planning

For Example

Activity	Team/Person	System	Stage	Next activity	Comments
Take order	Customer Service	IT / Manual	Collection	Order sent to warehouse or to local store	
Locate items	Dispatch, w/h	IT / Manual	Primary	Items to local store for delivery	
Notify customer	Customer Service	IT / Manual	Primary	Customer pays and collects	Promo to mobile (Sales)
Promo texts to mobile	Sales	IT / Manual	Secondary	Promo to mobile	

In large organisations, Auditors may request Departmental organisational Charts to determine reporting lines & Responsibility Areas

Risk Assessment: Planning



3. Get Answers to Questions

Personal Data		Name of Assessor/date(s)					
Activity	Who	What	Why	Source	System	Date	Comments
Customer Order Taking	Customer Service	Full Name, Last Name, Address, mobile/landline	Order collection	Customer	Cust. Service IT	01/02/2017	
Promo Mechanics	Sales	Mobile	Promotion	Customer Service IT	Cust. Service IT	13/03/2017	Freq: varies

1st Principle, 2nd Principle (S19, S20) and 3rd Principle

Risk Assessment: Planning other areas

- Data Protection Registration
- 7th Principle
  - *Section 30: Data Processor*
  - *Section 31: Notification of Personal Data Breaches*
- 8th Principle: Data Subject Participation
- Special Personal Data: Higher Level of risk of harm
- Regulated Professions
- IT / Manual Systems

Risk Assessment: Identify Potential Risk

Go through each documented activity, study the questions, answers and the relevant Principles

Risk Assessment: Identify Potential Risk

- Is there any aspect of the **processing* of personal data that contravenes the relevant Principles?
- Could the personal data be **processed* in any other unexpected way that contravenes any of the relevant Principles?

**Processing: collection, storage, accessing, usage, disclosure, disruption, modification, perusal, inspection, or destruction of data*

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Identify Potential Risk

- 1st Principle: Lawful & Reasonable
- 2nd Principle:
  - S19 - Necessary, Relevant & Not Excessive
  - S20 - Prior Consent
- 3rd Principle: Specific, Lawful Purpose & Data subject must be aware

Risk Assessment: Identify Potential Risk

For Example

Personal Data Risk Assessment Pl			Name of Assessor/date(s)					
Activity	Who	What	Why	Freq	Source	System	Date	Comments
Taking Customer Order	Customer Service	First Name. Last Name, Address, Mobile/Landline	Order collection	N/A	Cust	Cust IT	01/02/2017	
Texts to Mobile	Sales	Mobile	Promotion	Varies	Cust IT	Cust IT	13/03/2017	

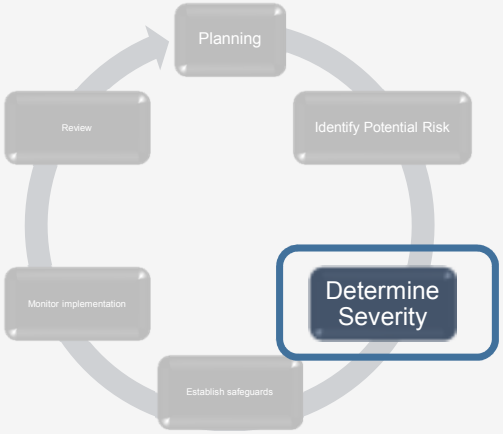
Risk Assessment: Identify Potential Risk

Examples

- Promotional texts sent to customer mobile
  - texts sent too frequently?
  - texts sent at inconvenient time or day?
  - irrelevant texts sent?
  - texts sent without prior consent?

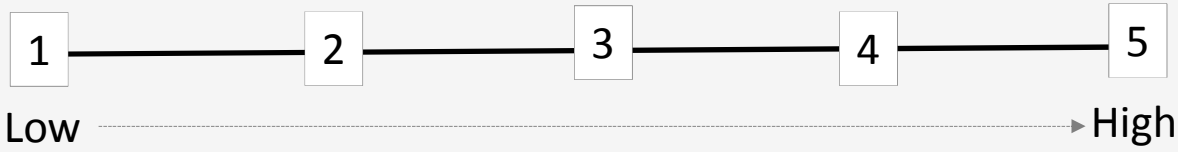
- Could the customer's contact details be used in any unexpected way?
  - To send promotional info in post?
  - To phone and inform them of promotions?
  - Any other way?

Risk Assessment: Determine Severity



Assign Severity level from Low to High Risk

- Scale System



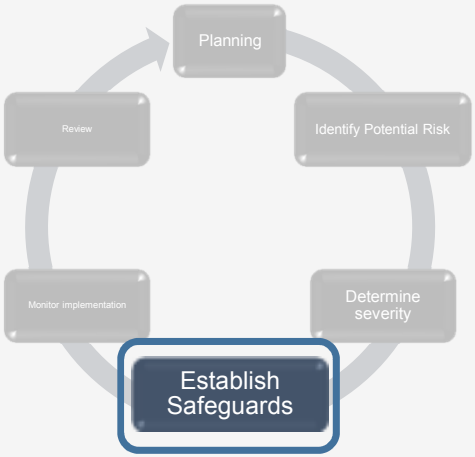
- Traffic Light System

Low Risk Medium Risk High Risk

Example: sending product promotional information to mobile devices: Risk – Low or High?

Dependent on different factors (time, day, frequency, nature/relevance of promotional material, consent et-c.)

Risk Assessment: Establish Safeguards



7th Principle: Data Controller should

- Regularly Verify that the Safeguards are effectively implemented
- Ensure that Safeguards are continually updated in response to new risks or deficiencies.
- Monitor Safeguards initial implementation
  - Ineffective safeguards? Investigate. Different course of action or tougher measures may be required.
  - Planned / frequent subsequent reviews
- Review Safeguards in response to new risks
  - Be aware of internal/external changes – may introduce new risks

Risk Assessment: Establish Safeguards

Technological Safeguards

- Role-based access control
- Email and network monitoring
- Business continuity – Backup, disaster recovery, ‘in the Cloud’ et-c
- Secure disposal of hard-disks
- Access control on door of offices with special data.

Organisational Safeguards

- Information Security/Privacy/ Data Protection Policy
- Data protection training for staff
- Clarity over roles/responsibilities
- Designated Data Protection Supervisor
- Guidance on good practice

NTSS Solutions

2017 DATA PROTECTION CONFERENCE

Risk Assessment: Establish Safeguards

Risk Assessment undertaken by					Dates	
Activity	Who	Potential Risk	Severity	Safeguards	Dates	Revised Severity
Promotional Texts sent to Customers' mobile	Sales	Sent Frequently Inconvenient Time / Day Irrelevant Text Without Prior Consent		On collection of data, get consent to send relevant promotions from time to time – Text sent no more than once /month – To be sent during office hours on Monday-Friday – Produce good practice guidelines & training – Customer IT System – checkbox for consent when personal data is collected – Promotion – relevant to products purchased		

Wishing you all a successful Data Protection

Audit in your various organisations

…

NTSS Solutions

2017 DATA PROTECTION CONFERENCE