Table of Contents

1.0 Purpose

The purpose of this document is to provide guidance to ensure that Information Asset and risk management process, allows risks to be identified, evaluated, proactively managed and reported effectively. This guidance document includes the risk register, risk impact and likelihood categories, and formalised lines of risk reporting to key decision makers.

2.0 Scope

a. From: Identification of Information Assets.

b. To: Risk Assessment, control and monitoring of risks.

3.0 References

Nil

4.0 Definitions

Risk Analysis- The process of identifying the potential impact of unwanted events and the likelihood of their occurring

Risk Assessment-The output from the Risk Analysis process

Risk Management- The entire process of identifying, documenting and evaluating risks and applying appropriate countermeasures to enable cost-effective security management and control.

Assets- At the highest level this is understood to mean anything that is of value to an organisation. This will include, for example, any form of computer hardware or software, networks, buildings, information (electronic and non-electronic, power supply, air-conditioning and personnel.

Impact-The consequences of an unwanted incident (either accidental or deliberate, or acts of God) affecting a set of one or more assets.

Threat- A potential violation of security. Threats may be environmental (e.g. earthquake or floods) or of human origin (accidental or deliberate).

Vulnerability-A characteristic or property of an asset or group of assets which can be exploited by a threat (i.e. a weakness that makes it easier for the threat to permeate) to cause loss or damage.

Risk: This is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset (I.e. an impact).

Countermeasure -A mechanism or procedure that reduces risk. Note that within the context of security management, the terms safeguard, countermeasure and control all have the same meaning.

Residual risk-The level of risk that remains after a justified (e.g. cost effective) set of controls have been implemented.

Confidentiality-The restriction of access to information by authorised persons, entities and processes at authorised times and in an authorised manner.

Integrity- Safeguarding the accuracy and completeness of information and information processing systems.

Availability-Ensuring that authorised users have access to information and associated assets when required.

5.0 Responsibilities

Document Owner:- The document owner of the document is responsible for obtaining the necessary authorisation/approval.

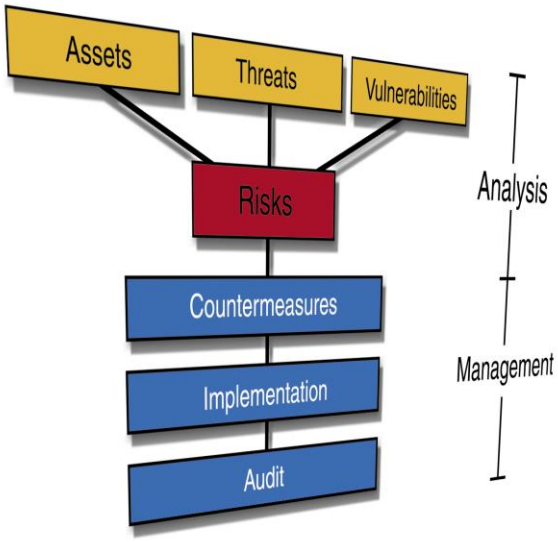
Asset Owner- The Asset owner is responsible for undertaking a CIA Assessment and reviewing periodically.

IT Manager/QA & Compliance Manager – The IT Manager/QA& Compliance Manager is responsible for reporting key findings and recommendations of risk assessments to the accountable Information Risk owner and also the Information Security Management Committee, are for ensuring risk treatment plans are regularly reported and tracked through to closure.

Assigned Risk Owner -The Owner of the Risk is responsible for documenting, implementing and maintaining controls identified to address the risk and support the ISMS on behalf of the Approver.

6.0 Overview

Below shows on the right is a visual diagram on the entire process. Risk is normally defined as the chance or likelihood of damage or loss. In this definition is extended to include the extent (impact) of damage or loss. That is, it is a function of two separate components, the likelihood that an unwanted incident will occur and the impact that could result from the incident. Having determined the various degrees of risk, DigiPlex is able to draw on its comprehensive library of countermeasures and recommend a balanced set of controls appropriate to the risk.

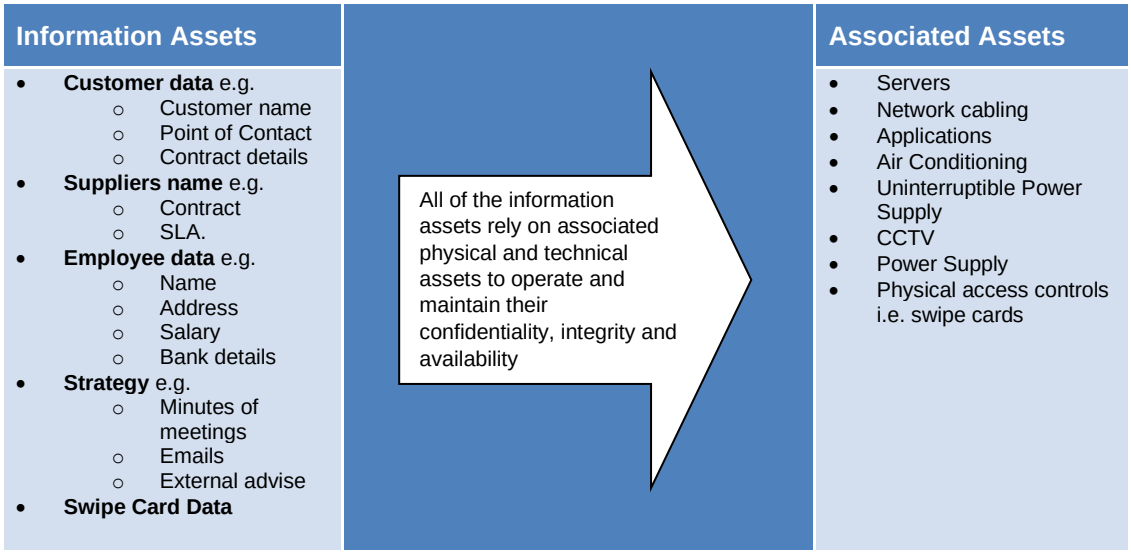


7.0 Procedure

The Assets identification and Risk Management process is illustrated diagrammatically in IT-PROC-01-00-DGS. The main elements of the Assets Identification and Risk Management process are described below.

7.1 Identify Information Assets

Information assets within DigiPlex business systems are identified from a number of sources and the below is an example and not exhaustive:-



Information and Associated Assets need to be assessed by the Asset Owner. It is possible that the associated assets support many information assets in which case their collective impact if there is a breach is much higher.

7.2 Impact Assessment of Assets

The Asset Owner will evaluate the impact on the Asset in terms of a breach of the data's Confidentiality, Integrity and Availability using the criteria set below and record on the Assets and Risk Register, IT-PROC-01-01-DGS.

Each asset should be assessed individually with the help of the IT Manager/QA and Compliance Manager. Once completed notify the QA & Compliance Manager/IT Manager so that the Risk Register can be updated and a Risk Assessment can be undertaken if required.

Each asset that is identified from the CIA assessment as “Very Low/Low”, is added to the risk register, accepted automatically, greyed out, the date of its acceptance inputted and the date for review added.

The definitions of CIA are detailed in the tablebelow.

Business Impact	**Impact rating for every impact category (direct financial loss, reputational damage, legal and regulatory obligations and strategic & commercial interests).**
Confidentiality	Potential loss that could arise due to unauthorized disclosure of data.
Integrity	Potential loss that could arise from a breach of the system's data accuracy.
Availability	The loss that would be suffered by the DigiPlex in case of the system being unavailable following a major failing.

The following table details the impact category headings along with the consequence of a breach to give an impact level. e.g. What would be the financial and reputational impact on DigiPlex if the data was leaked (i.e. confidentiality impacted)

Impact scores			
	Impact Category Definitions (Effect categories)		
Qualitative Assessment and Impact	**Confidentiality –** **Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.**	**Integrity –** **Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity**	**Availability-** **Ensuring timely and reliable access to and use of information**.
Very High (5)	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals. Major Legal / Regulatory failure resulting in legal proceedings or regulatory fines.	The unauthorised modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals. Major Legal / Regulatory failure resulting in legal proceedings or regulatory fines.	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 organisational operations, organisational assets, or individuals. Major Legal / Regulatory failure resulting in legal proceedings or regulatory fines.
High (4)	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals. Significant Legal / Regulatory resulting in potential legal action against DigiPlex or one of its Employees.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals. Significant Legal / Regulatory resulting in potential legal action against DigiPlex or one of its Employees.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals. Significant Legal / Regulatory resulting in potential legal action against DigiPlex or one of its Employees.
Medium (3)	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals. Material legal or regulatory failure	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals. Material legal or regulatory failure	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals. Material legal or regulatory failure

Low (2)	The unauthorised disclosure of information could be expected to have a **little adverse** effect on organisational operations, organisational assets, or individuals or individuals with minimal legal or regulatory impact	The unauthorised modification or destruction of information could be expected to have a **little adverse** effect on organisational operations, organisational assets, or individuals or individuals with minimal legal or regulatory impact	The disruption of access to or use of information or an information system could be expected to have a **little** adverse effect on organisational operations, organisational assets, or individuals with minimal legal or regulatory impact
Very Low (1)	The unauthorised disclosure of information could be expected to have a **No** adverse effect on organisational operations, organisational assets, or individuals or individuals and No Legal or Regulatory Impact	The unauthorised modification or destruction of information could be expected to have a **No** adverse effect on organisational operations, organisational assets, or individuals or individuals and No Legal or Regulatory Impact	The disruption of access to or use of information or an information system could be expected to have a **No adverse** effect on organisational operations, organisational assets, or individuals and No Legal or Regulatory Impact

7.3 Risk Assessment

The IT Manager/QA & Compliance Manager will undertake a Risk Assessment using the Assets and Risk Register. IT-PROC-01-01-DGS assets that have a CIA score level of "Medium" or higher are further risk assessed utilising the Threat and Vulnerability assessment. Further guidance is available in IT-PROC-GUI-01-02-DGS. All other assets are assessed in terms of the liklihood threats and vulnerabilities

7.3.1 Threats

A threat can be described as a situation or event that has the potential to cause harm i.e. disclosure, modification or destruction of a data asset or to data processing resources. Further guidance is available in IT-PROC-GUI-01-02-DGS.

Threats can be:

- People, Programmatic or Natural (Environmental)
- And can be external or internal for example: External hackers, insiders attackers, misuse, system failures, malware attacks (Trojans, virus etc) fire, flood, lighting strike major incident (national emergency, terrorist attack etc)

7.3.2 Vulnerabilities

Vulerabilities are weaknesses in computer security systems and environments that can be exploited in various ways by threats. These could be design weaknesses or lack

of maintenance (patching) through to lack of protection against intrusion or natural events.

Vulnerabilities can be inherent to a systems or software or caused or created by people or based on environmental or geographical location. Further guidance is available in IT-PROC-GUI-01-02-DGS.

Examples:

- Systems not patched against OS or software vulnerabilities or AV
- Insufficient perimeter controls
- Insufficient internal access control (authentication/ authorisation)
- Lack of resiliance (back up, hot standby, offsite storage, single points of failure, inadequate succession planning)

7.3.3 Current Controls

Before the scales for Threats and Vulnerabilities are assessed, the current controls DigiPlex has in place are considered in terms of how they reduce the vulnerabilities. Further guidance is available in IT-PROC-GUI-01-02-DGS.

7.3.4 Probability

For each threat / vulnerability scenario, the likelihood of compromise shall be calculated using the guidelines within the following table. Existing security controls and vulnerabilities shall be taken into account when considering the likelihood of each threat occurring.

Probability scores		
Qualitative Assessment for Probability /Likelihood	**Probability / Likelihood**	**Occurrence of damage**
Almost Certain (5)	>80%	More than once a year
Likely (4)	61-80%	Once every 1 - 2 years
Moderate (3)	41-60%	Once every 2 - 5 years
Unlikely (2)	20-40%	Once every 5 - 10 years
Rare (1)	<20%	Less than once every 10 years

Probability scores should be means tested (or common sense tested) to ensure that risk impacts relate accurately to real world perceptions of the risk. Probability score produces the probability multiplier used to populate the Probability x Impact equation to produce the final risk score.

7.3.5 Calculating the Risk Rating

The following example demonstarted how the risk rating is calculated using the table in 7.3.4 and the risk reguster, IT-PROC 01-01-DGS

Example:

THREAT/ VULNERABILITY =3 (PROBABILITY)

7.3.5.1 Impact

Using the impact assessment detailed above, re-evaluate the CIA impacts based on the existing controls that are now known to be in place to combat the identified threats and vulnerabilities. In this model the maximum of the three scores is taken and used as the Impact . Risk impact scores must be accurate and approved by accoutable owner.

Example:

IMPACT 1 -5			
CONFIDENTIALITY	INTEGRITY	AVAILABILITY	MAXIMUM
5	5	4	5

7.3.5.2 Risk Rating Score

The risk is calculated by multiplying the Probability and Impact scores.

Example: Probability 3 x Impact 5 = Risk 15

Risks are categorised into risk levels based on scores as follows:

			Impact				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Probability	Rare	1	1	2	3	4	5
	Unlikely	2	2	4	6	8	10
	Moderate	3	3	6	9	12	15
	Likely	4	4	8	12	16	20
	Almost Certain	5	5	10	15	20	25

Very High= Red= 21-25

High= Orange =12-20

Medium =Yellow=4-11

Low- Green=1-3

7.4 Risk Treatment Plan

The risk of treatment criteria provides a framework for risk assessment review and formulation of risk treatment plans.

The Risk Treatment Plan identifies the controls that are needed to address each of the identified risks from the risk assessment. It defines how, based on the criteria established by ISMC, each risk is to be handled, who it is assigned to and how progress will be monitored and reported.

7.5 Risk Appetite

The following table defines DigiPlex's risk appetite and defines the action required and the review frequency .

Risk Level	Comment	Action	Review Frequency
Very High 21-25	No very high risk can be tolerated or accepted	Any such critical risk must be treated immediately and added to the Risk Treatment Plan (RTP) Reduce/ Accept and Escalate by Chair	By the Compiance & Assurance Director on a monthly basis.
High 13-20	Can be accepted by the Site Manager. If they are not accepted then the additional controls required	Not accepted risks need to planned to reduce within 12 months and added to the RTP.	Review at quarterly intervals.
Medium 4-12	Can be accepted by the Risk Owner. If they are not accepted then the additional controls required	Not accepted risks to planned to reduce within 12 months and added to the RTP.	Review at six monthly intervals.
Low 1-3	Risks are automatically accepted	Note in the risk register risk when risk will be reviewed.	Review annually

This process for accepting or treating risks must comply with DigiPlex current risk appetite and strategy i.e. Very High risks must result in notification and approval by the Senior Management Team.

Assets rated as a " High" and "Medium" need to be either accepted or the Compliance and Assurance Director may decide to reduce the risk. Risks can be treated in various ways:

- Avoid – Cease the activity that produces the risk.
- Mitigate – Employ countermeasures to reduce the risk.
- Transfer – Seek alternative strategies to cover the potential loss should the risk occur i.e. insure against the loss.
- Accept – The level of risk is acceptable to the business, in other words management deem the risk acceptable, compared to the cost of improving controls to mitigate it.

The residual risk figure is used to estimate the level of risk potential following implementation of the Risk managment strategy. Subsequent risk assessments will use this figure as a baseline to monitor the effectiveness of the controls being implemented to reduce identified risks to the acceptable levels.

7.6 Review

The Asset register and risk register will be reviewed by Asset and Risk Owners at the required review dates and reviewed by the ISMC at meetings to ensure that all relevant assets, vulnerabilities threats and risks remain accurate.

The following events will trigger a review of the Assets and Risk Register:-

- A Seroius Incident
- Change in Legisation
- Change of Asset
- Internal Audit

Once risk treatments are completed the Statement of Applicablity (SOA), IT-PROC-01-02-DGS will be updated to document the controlsand the revision status will be revised by the IT Manager.

8.0 New Asset and Risk Identification

Annually in October an entire review of the Asset register will be conducted to ensure all relevant assets, vulnerabilities and threats have been identified and considered. In addition the risk register will be reviewed to establish if any new risks can be identified.

9.0 Measurement

Measurement of this process is by analysis of performance data discussed at meetings:

- New Risks Added (This Period)
- Risks Closed (This Period)
- Total Open Risks (Cumulative)
- Total Closed Risks (Cumulative)
- Verison of SOA

10.0 Forms and Templates

The following forms and templates are an integral part of this procedure.

Asset and Risk Register	IT-PROC-01-01-DGS
Statement of Applicability	IT-PROC-01-02-DGS
Guidance on Threat Vulnerabilities & Controls	IT-GUI-01-02-DGS

11.0 Records and Retention

Controlled documents that have been superseded or withdrawn will be archived as specified in the latest issue of the Control of Records procedure