

Risk Assessment Procedure

Version number: 1.0

Publish date: 16-05-2018

Document control	
Prepared by	Mike Moore, Managing Director
Authorised by	Upper Management
Physical Copy location(s)	Operations Folder
Source Copy Location(s)	Dropbox - GDPR123\Documents\Final Documents
Published Copy Location(s)	www.Dephoto.biz\GDPR
Other Referenced Documents	
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	Risk Assessment Procedure			
Description	To assess risks in such situations where risk needs to be considered and mitigated.			
Created by	Mike Moore			
Date Created	16-05-2018			
Maintained by	Upper Management			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	Mike Moore	First creation	16-05-2018	Published

Contents

Purpose	3
Prerequisites	3
Conditions	3
Outcomes.....	3
Processes	4
Identifying a risk sub-process.....	4
Carrying out a risk assessment sub-process	4
Reporting risk assessment results if there are risks exceeding the risk assessment sub-process.....	6
Reporting risk assessment results if there are no risks exceeding the risk appetite sub-process.....	6
Management and Review.....	6

Purpose

This procedure is to be used to allow appropriate parties to assess risks in such situations where risk needs to be considered and mitigated. DE Photo (Franchising) Ltd (referred to as the company here after) information security management systems uses a risk based approach to ensure there is sufficient protection in place to meet the information security standards and so this procedure should be followed when there is a change to the company's systems, devices, networks, operations, policies, procedures or obligations.

Prerequisites

For this procedure to be followed the following conditions need to be met:

- All parties need to be aware of their roles and responsibilities.
- The risk assessment master template needs to be current and available to the relevant parties.
- Any systems/services/devices referenced need to be available to the relevant parties.
- All parties have had the relevant training and the training is current and up to date.
- Documented controls and measures are in place to allow swift reporting of incidents.

Conditions

This procedure should be followed when there is a need to perform a risk assessment. Some examples of this would be:

- Performing a data protection impact assessment.
- Determining security controls.
- Proposing a change

Outcomes

Risk Assessment is completed and reported

Risk Assessment is logged and stored

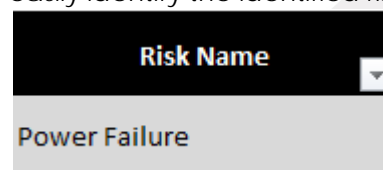
Processes

Identifying a risk sub-process

1. Considering how data is processed, derive all the ways unauthorised parties could gain access to data. These should be considered risks and included in a risk assessment.
2. Considering how data is processed, derive all the ways the integrity of data could be affected. These should be considered risks and included in a risk assessment.
3. Considering how data is processed, derive all the ways the data could be rendered unavailable. These ways should be considered risks and included in a risk assessment.
4. Where the assessor does not have sufficient knowledge, perform the assessment. An approved expert should be relied upon.

Carrying out a risk assessment sub-process

1. Open the risk assessment template stored at :
Dropbox: \GDPR\Documents\
Save a copy of this template to
Dropbox: \GDPR\Documents\File Locations\Rectification Request
with name convention:
[Branch]-[Surname]-[Date]-[Doc Number]
for example HO-Moore-16-05-2018-001
2. Go to the risk table sheet and fill in the following information for each identified risk:
 - a. Risk Name – A name to easily identify the identified risk.



A screenshot of a dropdown menu. The top bar is black with the text "Risk Name" in white. Below it, a grey box contains the text "Power Failure". A small downward-pointing arrow is visible on the right side of the grey box.

Figure 1.1: Example of a risk name.

- b. Risk Likelihood – the chance that the risk would occur in a period of 12 months as a percentage.



A screenshot of a dropdown menu. The top bar is black with the text "Risk Likelihood (%)" in white. Below it, a grey box contains the text "50.00%". A small downward-pointing arrow is visible on the right side of the grey box.

Figure 1.2: Example of risk likelihood

- c. Estimated impact – Use the impact to choose an appropriate value based on the estimated cost of fixing the results of the risk. These costs will need to cover replacing and repairing affected systems/devices/networks, paying fines, legal costs, time costs, reputational damage repair costs and any other appropriate costs.

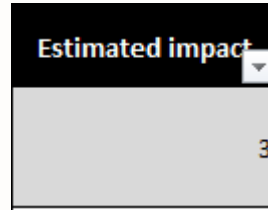


Figure 1.3: Example of estimated impact

- d. Description of risk – Details threat and possible consequences.

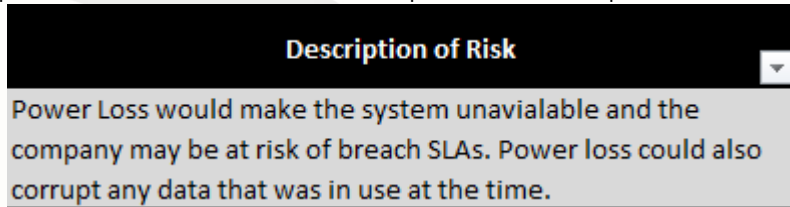


Figure 1.4: Example of description of risk

- e. Possible treatments – Details of actions that can be taken to lessen or remove the risk

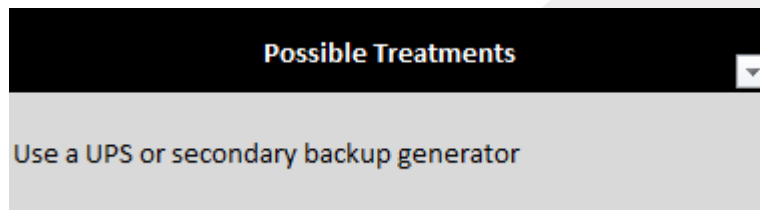


Figure 1.5: Example of possible treatments

3. Once the fields are populated, enter your name and the date the assessment was completed at the bottom of the table in the spaces provided, print a copy and store it in the risk assessment section of the confidential folder.
4. Save the changes.

Reporting risk assessment results if there are risks exceeding the risk assessment sub-process

1. The risk assessment is saved to:
Dropbox: \GDPR\Documents\File Locations\ Risk Assessments Completed
2. The project owner and information security dept. is informed of the results via an encrypted email.

Reporting risk assessment results if there are no risks exceeding the risk appetite sub-process

1. The risk assessment is saved to:
Dropbox: \GDPR\Documents\File Locations\ Risk Assessments To Be Actioned
2. The project owner is informed of the results via an encrypted email.

Management and Review

This policy should be reviewed as scheduled once annually unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16/05/2018

Next Review Date: 16/05/2019