[Organization logo]

[Organization name]

Commented [20A1]: All fields in this document marked by square brackets [ ] must be filled in.

RISK MANAGEMENT POLICY

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Commented [20A2]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	20000Academy	Basic document template

Table of contents

1. Purpose, scope and users

The purpose of this policy is to ensure that risks and opportunities of [organization name] are managed through an established process.

This document is applied to all activities, processes, and documents included in the SMS.

Users of this document are all employees of [organization name], as well as all relevant external parties who have a role in the SMS.

2. Reference documents

- ISO/IEC 20000-1:2018, clauses 8.5.1
- SMS Plan
- IT Service Continuity Management Process
- Availability Management Process
- Information Security Management Process
- Supplier Management Process
- Change Management Process

3. Policy

3.1. Scope and goals of risk management

[Organizations name]'s risk management [illegible]

The goals of risk management are to:

- [illegible]
- [illegible]
- [illegible]
- [illegible]

3.2. Process guidelines

[illegible]

The detailed description of the process is documented below:

3.2.1. Identification & Recording

[illegible]

- [illegible]

Commented [20A3]: Please include the name of your company.

Commented [20A4]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "04_SMS_Plan"

Commented [20A5]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "11_Service_Assurance_Processes/11.2_IT_Service_Continuity_Management"

Commented [20A6]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "11_Service_Assurance_Processes/ 11.1_Service_Availability_Management".

Commented [20A7]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "11_Service_Assurance_Processes/ 11.3_Information_Security_Management".

Commented [20A8]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "07_Relationship_Agreement_Processes/07.3_Supplier_Management".

Commented [20A9]: You can find a template for this document in the ISO 20000 Toolkit folder ISO 20000 Toolkit folder "09_Service_Design_Build_Transition_Processes/09.1_Change_Management".

Commented [20A10]: These are just best practice examples. You can delete some or include additional goals according to your company practices.

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Whenever a new risk is identified [illegible]

Whenever a new opportunity is identified [illegible]

3.2.2. Assessment

Once the risks have been identified, [illegible]

Impact Assessment:

Low impact	0	[illegible]
Moderate impact	1	[illegible]
High impact	2	[illegible]

Probability Assessment:

Low probability	0	[illegible]
Moderate probability	1	[illegible]
High probability	2	[illegible]

Commented [20A11]: E.g. Service Continuity Management Process, Information Security Management Process, Service Availability Management Process, Supplier Management Process, Change Management Process.

Commented [20A12]: [illegible]

Commented [20A13]: [illegible]

Commented [20A14]: These are only recommendations; you can adapt them according to your company practices.

The risk owner records the results of the risk assessment in the Risks and Opportunities Register (in the "Risk" worksheet).

The assigned Risk owner will prepare an estimation of the actual costs for any identified opportunities. [job title] will document the costs in the Risk and Opportunities Register (in the "Opportunity" worksheet).

Commented [20A15]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager, etc.

3.2.3. Evaluation

The following risk acceptance criteria are to be used by the assigned risk owner when evaluating the risks: Values 0, 1, and 2 indicate acceptable risks, while values of 3 and above indicate unacceptable risks.

Commented [20A16]:

3.2.4. Treatment

Each unacceptable risk must be treated. The assigned risk owner must decide on a risk response measure for each unacceptable risk. [job title] must introduce in the Risk and Opportunities Register the risk response measure and a detailed explanation of the measure. Risk response measures may include:

Commented [20A17]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager, etc.

- Implementing controls to reduce the risk level
- Partial transferring of risk to third parties (via insurance or outsourcing)
- Avoidance of risk (giving up on certain activities that introduce the risk, but with the caveat of losing any opportunities associated with those activities)

If the risk response involves the implementation of a control, [job title] will document the chosen control(s) in the Risks and Opportunities Register ("Controls" worksheet).

Commented [20A18]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager, etc.

The assigned opportunity owner will evaluate any identified opportunities based on the estimated cost and the expected benefits of the opportunity and will decide on a response measure based on the results of the evaluation. [job title] will document the response measure in the Risk and Opportunities Register.

Commented [20A19]:

3.2.5. Monitoring

For any new risks and opportunities documented in the Risks and Opportunities Register, [job title] will notify the selected risk/opportunity owners as soon as the Risks and Opportunities Register is updated.

The risk/opportunity owners are responsible for monitoring and reporting quarterly on the status of the risk/opportunity to [job title].

Commented [20A20]: company practices.

Commented [20A21]:

4. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

Commented [20A22]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager, etc.

Commented [20A23]: This is only a recommendation; please adjust the frequency according to your company practices.

5. Managing records kept on the basis of this document

Record name	*Storage location*	*Person responsible for storage*	*Controls for record protection*	*Retention time*
Risks and Opportunities Register	[tool name]	[job title]	[job title]	[...]

Commented [20A24]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager etc.

Commented [20A25]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, Risk Manager etc.

Commented [20A26]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

6. Appendices

- Appendix 1 – Risks and Opportunities Register

[Job title]
[Name]

_____
[Signature]

Commented [20A27]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.