Report on the ICT risk management framework review

A practical template for preparing the report on the ICT risk management framework review

A template by NOREA

Authors:

Stef Smit – Kouters Van der Meer

Marvin Kruin – MNK Risk

Jesper de Boer – Deloitte

Sandeep Gangaram Panday - Brightlyn

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl

Taskforce reviewers
The template was reviewed by the following members of the NOREA Taskforce Regulatory:

Name	Role	Company
Andrey Prozorov	Cyber security & Privacy expert	ISMS PRO
Danny Bos	Senior manager Cybersecurity & Privacy	Eraneos

The template was developed in collaboration with Kouters Van der Meer.

For the full member list and more content created by the Taskforce, please see https://www.norea.nl/dora or follow us on LinkedIn: https://www.linkedin.com/showcase/taskforce-dora

Table of contents

0 Reading guide

This template has been developed by NOREA, the professional association for IT auditors, to support organizations in preparing the report on the ICT risk management framework review in line with Article 6(5) of Regulation (EU) 2022/2554 (DORA) and Article 27 of the RTS on ICT Risk Management. It is intended as a practical aid to structure, document, and communicate the outcomes of the review in a consistent and comprehensive manner.

The template is designed to be used as a baseline document. Standardized wording, guidance text, and example formulations are provided in **black** to support consistent interpretation and application. These can be adopted directly or tailored to fit the specific context of the organization. Elements, to be described by the user, reflecting mandatory DORA requirements are indicated in **green** and should be completed to ensure regulatory alignment. Additional elements marked in **blue** represent recommended practices that, while not required under DORA, contribute to a more robust and mature ICT risk management framework and are therefore encouraged.

Organizations are expected to complete, adapt and validate the template based on their own governance structure, risk profile and context. The template should not be treated as a checklist to be followed mechanically. Rather, it should be used as a structured guide that supports professional judgement and organization-specific interpretation of DORA requirements.

Disclaimer

This template is provided for guidance purposes only. While it has been developed with due care and professional expertise, NOREA does not guarantee completeness, accuracy, or suitability for any specific organization or regulatory context. The responsibility for ensuring compliance with DORA and other applicable laws and regulations remains solely with the organization using this template. Users are expected to perform their own assessment and, where necessary, seek independent professional or legal advice.

While this template can offer valuable insights, it is important to note that the legal requirements set out in DORA itself remain leading.

[logo of the financial entity]

Report on the ICT risk management framework review

[name of the financial entity]

[review period start – review period end]

Document control

Field	Details
Report version	V [X.X]
Date of drafting	[DD/MM/YYYY]
Date of management body approval	[DD/MM/YYYY]
Function responsible for the review	[e.g. CISO]
Classification	[e.g. confidential / internal]

Prepared in searchable electronic format in accordance with Article 6(5) of Regulation (EU) 2022/2554 (DORA) and Article 27 of the RTS on ICT Risk Management

1 Introduction

As part of its ICT risk management framework, [financial entity] (hereinafter: ["abbreviated name" or "the financial entity"]) performs an annual review of the ICT risk management framework. This review enables [financial entity] to progressively enhance the maturity of its ICT risk management framework by identifying areas for improvement and acting upon them. The management body retains ultimate responsibility for the adequacy and effectiveness of the ICT risk management framework.

This report has been prepared based on information sources including [describe information sources listed in chapter 8]. Through this report, which is approved by [financial entity]'s management body as part of its oversight responsibilities regarding ICT risk management and digital operational resilience, [financial entity] complies with the requirements as set out in Article 6(5) of Regulation (EU) 2022/2554 (DORA) and Article 27 of the RTS on ICT Risk Management.

This report further elaborates on the activities performed in relation to the ICT risk management framework, the evaluation of that framework, and the corrective measures to be acted upon. This report has been prepared by [function responsible for review] under responsibility of the management body of [financial entity]. This report has been prepared [as part of the regular ICT risk management framework / upon the occurrence of a major ICT-related incident (list all ICT-related incidents with incident root- cause analysis) / following supervisory instructions (reference the instructions) / following conclusions derived from relevant digital operational resilience testing (reference the conclusions) / following conclusions derived from relevant audit processes (reference the conclusions)].

1.1 Executive summary

[briefly summarize the findings, corrective measures and conclusions of this report]

1.2 The financial entity and its context

Subject: [describe the financial entity that is the subject of the report, including its full legal name, LEI code, registered address, supervisory authority and where relevant, describe its group structure]

Context: [describe the nature, scale and complexity of the financial entity's services, activities and operations]

Organization: [describe the organization and strategy of the financial entity]

Critical functions: [list the critical or important functions of the financial entity or summary and reference to complete list]

ICT environment: [describe the key in-house and third-party ICT systems and services and the impact of their loss or degradation]

Major ongoing projects or activities: [describe significant transformation, outsourcing or change programs relevant to ICT risk]

1.3 Summary of changes [since previous report / the past year]

[when there is a previous report present] Since the previous report, regarding [review period start – review period end], the most significant changes to the ICT risk management framework were:

[when this is the first documented report] In the past 12 months, the most significant changes to the ICT risk management framework were:

[Change 1]: [summarize the change and its impact on digital operational resilience in a few sentences]

[repeat for each change]

1.4 Summary of ICT risk

Current risk profile: [describe the current risk profile of the financial entity regarding ICT risk, referencing past risk assessments and business impact assessments when possible]

Near-term risk profile: [describe the near-term risk profile of the financial entity regarding ICT risk, referencing identified key emerging risks or anticipated changes when possible]

Threat landscape: [describe the threats to the financial entity identified during the review period]

Control effectiveness: [describe the effectiveness of the controls executed during the review period and the impact of the effectiveness on the risks of the financial entity in relation to its risk tolerance, including an assessment of whether control effectiveness is sufficient given the entity's risk appetite.]

Security posture: [describe the security posture of the financial entity regarding digital operational resilience]

[Governance and integration: describe how ICT risk management is integrated within the overall enterprise risk management framework, including roles, responsibilities, escalation mechanisms and alignment with business decision-making]

2 Major changes and improvements

As summarized in chapter 1.2, [since the previous report / in the past year], several changes and improvements have taken place. For each change or improvement, an analysis has been performed to assess its nature and impact on digital operational resilience, risk management, and governance, to provide insight into the effects on [the financial entity]. The analysis should include an assessment of how these changes contribute to improving the effectiveness and maturity of the ICT risk management framework.

2.1 Internal changes and improvements

[e.g. changes to the digital operational resilience strategy, the ICT internal control framework or ICT risk management governance, etc.]

- **[change or improvement]:** [describe the change or improvement, including: if it is a change or an improvement, its relevance for identified risks, control effectiveness and overall resilience posture, when it has taken place, how it was handled and what its impact was on the digital operational resilience, risk management, and governance of the financial entity]

  [repeat for each change and improvement]

2.2 External changes and improvements

[e.g. relevant emerging technologies, laws and regulations, industry best practices, etc.]

- **[change or improvement]:** [describe the change or improvement, including: if it is a change or an improvement, its relevance for identified risks, control effectiveness and overall resilience posture, when it has taken place, how it was handled and what its impact was on the digital operational resilience, risk management, and governance of the financial entity]

  [repeat for each change and improvement]

3 Findings of the review

This comprehensive review of [the financial entity]'s ICT risk management framework is grounded in a systematic analysis of evidence gathered from multiple internal and external sources. These sources provide foundational inputs that inform the identification of weaknesses, deficiencies, and gaps within our ICT risk management architecture. The review integrates findings from [e.g. first, second and third line control activities, operational incident data, and the outcomes of targeted resilience assessments], supplemented by [e.g. monitoring of the external threat landscape and emerging regulatory developments].

The following sources and inputs have been consolidated to support this review:

Internal Sources:

- [describe an internal source listed in chapter 8 of this report]
  [Repeat for each internal source]

External Sources:

- [describe an external source listed in chapter 8 of this report]
  [Repeat for each external source]

Internal and external sources of information are be included and described in more detail in chapter 8. To gather the findings of this review, [the financial entity] considers every key domain within its ICT risk management framework, evaluates their execution, analyses identified weaknesses, deficiencies and gaps and determines their severity and impact, including their relevance in relation to our risk appetite and business impact.

[key domains may include governance and risk management, operational management, continuity management, incident management, software and systems development, third-party risk management, resilience testing and security management]

Field	Details
Finding ID	[e.g. F-001]
Domain	[describe the domain(s) in which the finding occurred]
Description	[describe the weakness, deficiency or gap in detail]
Severity	[e.g. critical / high / medium / low, including the impact of the finding on business operations, critical functions or objectives]
Basis for Severity Assessment	[describe the methodology and rationale used to assess the severity]
Source	[describe the source(s) of information used to identify and analyze the weakness, deficiency or gap, including a reference to chapter 8]

[repeat for each finding]

4 Corrective measures

To address identified weaknesses, deficiencies, and gaps, [the financial entity] will implement the following measures:

4.1 Summary of measures

Finding ID	Measure ID	Measure description	Status	Priority
[e.g. F-001]	[e.g. M-001]	[summarize the measure]	[planned/ in progress/ completed]	[high / medium / low]
[e.g. F-001]	[e.g. M-002]	[summarize the measure]	[planned/ in progress/ completed]	[high / medium / low]
[e.g. F-002]	[e.g. M-003]	[summarize the measure]	[planned/ in progress/ completed]	[high / medium / low]

4.2 Detailed description of measures

Field	Details
Finding ID	[e.g. F-001]
Measure ID	[e.g. M-001]
Measure description	[describe the measure in detail]
Status	[planned/ in progress/ completed]
Target date	[expected date for implementing the measure, including its priority]
Control date	[expected date for internal control of the measure]
Current progress	[describe the current progress on implementing the measure]
Timeline risk	[explain, if applicable, if and why there is a risk that deadlines may not be respected]
Used tools	[describe, if applicable, internal and external tools to be used for this measure]
Responsible function	[describe the internal or external function responsible for this measure]
Impact	[describe the impact of the changes, including alignment with risk appetite and expected risk reduction, envisaged in the measures on the financial entity's budgetary, human, and material resources, including resources dedicated to the implementation of any corrective measures]
Authority notification	[describe, if applicable, the process for informing the competent authority]

[repeat for each measure]

4.3 Evaluating findings that are not subject to corrective measures

[if the financial entity will implement measures for every finding] Considering all identified findings are subject to corrective measures, [the financial entity] does not identify any findings that are not subject to corrective measures.

[if there are findings that the financial entity will not implement measures for] In addition to the identified findings that are subject to corrective measures, [the financial entity] analyses the residual risk for the following findings which are not subject to corrective measures:

Field	Details
Finding ID	[e.g. F-001]
Criteria for impact	[describe the criteria used to analyze the impact of the finding in detail]
Impact	[describe the impact of the changes envisaged in the measures on the financial entity's budgetary, human, and material resources, including resources dedicated to the implementation of any corrective measures]
Criteria for residual risk	[describe the criteria used to evaluate the related residual ICT risk]
Residual risk	[describe the related residual ICT risk]
Criteria for acceptance	[describe the criteria used to accept the related residual risk]
Acceptance	[describe the acceptance of the related residual risk]

[repeat for each finding]

4.4 Evaluating the ICT risk management cycle

[In addition to the identified findings and measures, the financial entity performs a reflective assessment of the effectiveness of the ICT risk management cycle. This assessment is based on interviews with all relevant stakeholders of the risk management including those charged with governance]:

[describe the evaluation based on design effectiveness, operational effectiveness, integration within organization, identified structural weaknesses, improvement opportunities, etc.]

5 Future developments

In addition to the changes and improvements detailed in chapter 2, [the financial entity] identifies and analyses planned and potential developments performed to assess their nature and potential impact on digital operational resilience, risk management, and governance, to provide insight into the potential effects of these developments on [the financial entity] and their relevance for risk exposure, control effectiveness and required prioritization of improvement actions

5.1 Internal developments

[e.g. changes to the digital operational resilience strategy, the ICT internal control framework or ICT risk management governance, etc. beyond identified improvement measures]

- **[Development]:** [describe the development, including its expected impact on risk levels, control requirements and prioritization of future measures when the development will take place, how the development will be handled and what its potential impact will be on the digital operational resilience, risk management, and governance of the financial entity]

  [repeat for each development]

5.2 External developments

[e.g. relevant emerging technologies, laws and regulations, industry best practices, etc. beyond identified improvement measures]

- **[Development]:** [describe the development, including its expected impact on risk levels, control requirements and prioritization of future measures when the development will take place, how the development will be handled and what its potential impact will be on the digital operational resilience, risk management, and governance of the financial entity]

  [repeat for each development]

6 Conclusions

Considering the executed review process, the described findings and corrective measures, [the financial entity] concludes that [provide the overall conclusions resulting from the review of the ICT risk management framework, which may include an assessment of maturity regarding internal or external frameworks, including an explicit overall judgement of the adequacy and effectiveness of the ICT risk management framework, a summary of key risks and control gaps and a forward-looking view on required improvements]

Overall judgement:
[adequate / partially adequate / inadequate / other classification defined by the financial entity]

7 Past reviews

[when this is the first documented report] There have been no previously documented review reports.

[when there is a previous report present] A list of the previously documented review reports is included below:

Report #	Review period	Date of approval	Reason for review
[e.g.1]	[start – end]	[DD/MM/YYYY]	[annual, following a major ICT-related incident, following supervisory instructions, etc.]
[e.g. 2]	[start – end]	[DD/MM/YYYY]	[annual, following a major ICT-related incident, following supervisory instructions, etc.]

7.1 Summary of past corrective measures

[when this is the first documented report] Since there have been no previously documented review reports, the are no past corrective measures to describe.

[when there is a previous report present] A list of corrective measures as a result from previously documented review reports is included below:

Report #	Measure ID	Measure description	Status	Target Date
[e.g.1]	[e.g. M-001]	[summarize the measure]	[describe the current state of implementation]	[DD/MM/YYYY]
[e.g.2]	[e.g. M-001]	[summarize the measure]	[describe the current state of implementation]	[DD/MM/YYYY]

7.2 Ineffective past corrective measures

[when this is the first documented report] Since there have been no previously documented review reports, there are no ineffective past corrective measures to describe.

[when there is a previous report present and all past corrective measures have proven effective and haven't created unexpected challenges] Since all past corrective measures have proven effective and haven't created unexpected challenges, there is no improvement to be made to them.

[when there is a previous report present and not all past corrective measures have proven effective or have created unexpected challenges] Regarding the overview of past corrective measures provided in chapter 7.1, the following corrective measures have proven ineffective or have created unexpected challenges:

Field	**Details**
Report #	[e.g. 1]
Measure ID	[e.g. M-001]
Issue	[measure has proven ineffective / measure has created unexpected challenges]
Description of the issue	[describe the issue in detail]
Improvement	[describe how the measure could be improved or changed to increase effectiveness or overcome challenges]

[repeat for each measure]

8 Sources of information

Throughout this review report, [the financial entity] has referenced used sources. These sources are listed and described in further detail below:

[sources should include the results of internal audits, the results of compliance assessments, the results of digital operational resilience testing, where applicable the results of advanced testing, based on threat-led penetration testing (TLPT), of ICT tools, systems, and processes and external sources]

Source	Description	Usage
[e.g. internal audit results]	[describe the source]	[describe the usage of the source regarding this review report]
[e.g. results of compliance assessments]	[describe the source]	[describe the usage of the source regarding this review report]
[e.g. results of digital operational resilience testing]	[describe the source]	[describe the usage of the source regarding this review report]