Risk Assessment & Management Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

Systematic risk assessments are important because they identify, prioritize, and help track the treatment of risks to CNTXT's commitments to its customers and other stakeholders. The purpose of this policy is to have a formalized risk assessment approach for risk identification, analysis, and treatment.

2. Scope

This document is applicable to all processes and operations in CNTXT within the scope of the ISMS.

3. Policy Statement

CNTXT periodically performs an operational risk assessment to identify risks impacting its commitments. Results from the assessment are compiled into a report reviewed by management. Identified security risks are risk-rated, assigned to a risk owner, and tracked to risk treatment completion or acceptance.

4. Risk Sources

Some common sources of risk are:

- The assessment considers internal and external security risk factors.
- Possibility of fraud affecting our ability to achieve our business objectives.
- Changes to the regulatory, economic, and physical environment in which the entity operates.
- Risks associated with third-party vendors. Please refer to the Vendor Management Policy for guidelines on assessing vendors.

5. Risk related concepts

5.1 Threats

A Threat is a possible situation or activity which may be deliberate, accidental, or caused by nature resulting in the degradation of the operational status of the organization. This may include but is not limited to service outages, data theft, physical harm, or financial loss.

5.2 Impact

Impact measures the extent of damage in the outcome of a threat event (usually loss or disadvantage). It represents the magnitude of harm expected from a fully materialized threat. Typical outcome scenarios for which the impact should be objectively measured are unauthorized access, unauthorized changes to data, unauthorized deletion of data, partial or complete loss of system availability, etc.

5.3 Likelihood

Given a threat, its likelihood measures the probability that the threat will occur “and” cause damage. Likelihood can be a qualitative description too. It should ideally combine the chance of the threat event being initiated and the chance that an initiated threat results in an adverse impact.

5.4 Risk Vulnerability

Risk vulnerability is a measure of the net harmful consequence of a given threat. It is measured by considering both the likelihood as well as the Impact of the given threat and calculated as below:

Risk = Impact * Likelihood (where * indicates multiplication)

5.6 Risk Assessment

A risk assessment is an exercise of making a list of all possible threats posed to the organization in the context of fulfilling its commitments to its customers and other stakeholders. It also measures the computed risk for each threat using the abovementioned method. Finally, the exercise benchmarks the computed risks against a predetermined acceptable risk level. Those threats above the acceptable level need to be addressed via mitigation measures.

5.7 Risk Management

Risk management is the program that implements risk assessment as described above and mitigation measures. It includes recognizing threats and risks, analyzing their likelihood and impact, treating and mitigating their outcomes, and monitoring the mitigation measures.

6. Risk Assessment Policy

- All CNTXT staff are responsible for identifying, analyzing, evaluating, monitoring, and communicating risks associated with any activity, function, or process within the scope of their responsibility and authority.
- Any staff member who spots a potential risk or vulnerability should report them to the information security team.
- All staff members are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible.
- Overall, the development and execution of risk assessments is the joint responsibility of CNTXT CEO, Information Security Officer, and the department or individuals responsible for the area being assessed.
- CNTXT performs periodic risk assessments using qualified internal staff or external third parties who have experience performing risk assessments.

- Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks.
- The risk assessment process and methodology will be updated as required in response to the results of audits and incidents.
- Management defines the scope of risk assessment and assembles the risk assessment team with an owner to guide the process (risk assessment lead).
- Given the scope, the risk assessment team then lists potential risks and threats to the system.
- For each threat, the impact of damage is quantified. We use a relative measure on a scale of 0 to 10, where 0 indicates minimal or negligible impact, and 10 indicates the maximum impact.
- For each threat, the probability or likelihood of occurrence is also computed. This can be quantified as a number between 0 and 1.
- The net risk of each threat is computed using the above two metrics. Net risk ranges between 0 and 10. Propose and recommend activities and controls to reduce the impact and likelihood of the threat.
- Create a risk assessment report using the above. Communicate the same to the management team. Also, communicate mitigation measures to the affected staff.
- Take risk mitigation actions and monitor their effectiveness.
- The risk assessment activity should be performed at least annually.
- It is important to consider the learnings from previous risk assessments. It is recommended to use these learnings to identify how threats to the organization are changing over a period of time and build proactive threat intelligence, which can be used in subsequent risk assessments.

7. Risk Mitigation

- When the net risk amounts to less than 3, there are very reasonable grounds to deem the risk acceptable.
- For higher risk values, the risk can still be considered acceptable if the cost of implementing mitigation measures exceeds the net dollar impact that might arise from the risk.
- If the risk cannot be mitigated, and the net risk exceeds 8, consider purchasing insurance as a protection measure. Consider the net dollar impact that might arise from the risk to evaluate the amount of insurance coverage.
- Threats/Risks shall be ranked in descending order of the net computed risk. This indicates the order of importance in which to address the threats. Controls are designed for the risks that have been selected to mitigate. A plan is created to implement the controls in this order.
- We then compute the “Residual risk” after fully implementing controls and mitigation strategies. One of the following decisions is made based on the residual risk:
    - Accept the risk.
    - Transfer the risk.

    - Add more controls.
    - Other actions as may be deemed necessary
- When the risk assessment report is completed, results shall be communicated to the affected business units and staff.

8. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

9. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

10. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Risk Assessment & Management Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024