



POLICY · GOVERNANCE

Risk Assessment and Management Policy

Version 1 · Approved by Jacek Janczura · 18 October 2026

Taufolio · Jacek Janczura
Adama Mickiewicza 73, 01-625 Warszawa, Poland
EU VAT: PL5253008276 · support@taufolio.com

Contents

1. Objective

2. Scope

3. Policy statement

4. Risk sources

5. Risk-related concepts

6. Risk assessment

7. Risk mitigation

8. Document security classification

9. Non-compliance

10. Responsibilities

11. Schedule

12. Version history

1. Objective

Systematic risk assessment identifies, prioritizes and tracks the treatment of risks to Taufolio's commitments to its users and other stakeholders. The purpose of this policy is to establish a formal approach to risk identification, analysis and treatment.

2. Scope

This policy applies to all processes and operations at Taufolio within the scope of the information security program, including the systems that hold customer brokerage credentials and personal data.

3. Policy statement

Taufolio periodically performs an operational risk assessment to identify risks that affect its commitments. The results are compiled into a risk register, kept by the Information Security Officer and reviewed by the owner of the business. Each identified risk must be rated, assigned a risk owner and tracked until its treatment is complete or the risk is formally accepted. The assessment must be performed at least annually and whenever a significant change occurs.

4. Risk sources

Common sources of risk that the assessment must consider include:

- internal and external security risk factors;
- the possibility of fraud, including account takeover and abuse of user accounts, affecting Taufolio's ability to meet its objectives;
- changes to the regulatory, economic and physical environment in which Taufolio operates, including data protection law and the rules of brokerage and AI providers;
- risks associated with third-party vendors and subprocessors (see the Vendor Management Policy);
- risks specific to the product, such as the compromise of customer brokerage credentials, errors in AI-generated content, and loss or corruption of portfolio data.

5. Risk-related concepts

5.1 Threats

A threat is a possible situation or activity, deliberate, accidental or natural, that degrades the operational status of the organization. Examples are service outages, data theft, physical harm and financial loss.

5.2 Impact

Impact measures the extent of damage caused by a threat event. It represents the magnitude of harm expected from a fully materialized threat. Typical outcomes to be measured are unauthorized access, unauthorized change of data, unauthorized deletion of data, and partial or complete loss of availability.

5.3 Likelihood

Given a threat, likelihood measures the probability that the threat will occur and cause damage. It may also be described qualitatively. Ideally it combines the chance that the threat event is initiated with the chance that an initiated threat results in an adverse impact.

5.4 Risk

Risk is the net harmful consequence of a threat. It is calculated by considering both its likelihood and its impact:

$\text{Risk} = \text{Impact} \times \text{Likelihood}$

5.5 Risk assessment

A risk assessment lists the threats to the organization in the context of its commitments to users and other stakeholders, computes the risk of each threat using the method above, and compares each risk with a predetermined acceptable risk level. Threats above the acceptable level must be addressed by mitigation measures.

5.6 Risk management

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

6. Risk assessment

- All staff members are responsible for identifying, analyzing, evaluating, monitoring and communicating risks associated with any activity, function or process within their responsibility and authority.
- A staff member who spots a potential risk or vulnerability must report it to the Information Security Officer by email.
- Staff members must cooperate fully with any risk assessment of the systems and procedures for which they are responsible.
- The development and execution of risk assessments is the joint responsibility of the owner of the business, the Information Security Officer and the people responsible for the area being assessed.
- Risk assessments may be carried out by qualified internal staff or by external specialists with relevant experience.

- The deliverables are an updated risk register and a risk reduction action plan that addresses every unacceptable risk.
- The assessment process and methodology must be updated in response to the results of audits and incidents.

The assessment proceeds as follows:

1. The owner of the business defines the scope of the assessment and names a risk assessment lead.
2. Within that scope, potential risks and threats to the systems and data are listed in the risk register.
3. For each threat, the impact is rated on a relative scale from 0 to 10, where 0 is negligible and 10 is the maximum impact.
4. For each threat, the likelihood is rated as a number between 0 and 1.
5. The net risk is computed from the two ratings. Net risk ranges from 0 to 10.
6. Activities and controls to reduce the impact and likelihood of the threat are proposed.
7. The results are recorded in the risk register and communicated to the owner of the business, and the mitigation measures are communicated to the affected staff members.
8. Mitigation actions are carried out and their effectiveness is monitored.

The assessment must be performed at least annually and on significant change, such as a new subprocessor, a new brokerage connector, a major architectural change or a security incident. Lessons from previous assessments and incidents should be used to see how threats change over time and to build proactive threat intelligence for later assessments.

6.1 Examples of tracked risks

The risk register tracks, among others, the following risks. Their treatments are described here as examples of how the method is applied.

- **Compromise of customer brokerage credentials.** An attacker obtaining the OAuth tokens, API keys or secrets that users grant Taufolio. Treatment: application-layer encryption of every credential before it reaches the database (AES-256-GCM with per-record keys bound to the user and the provider); the master key held outside the database in the hosting provider's secret store; a dedicated secrets table reachable only by server-side code; read-only brokerage scopes, so that credentials cannot be used to trade or move funds; server-only database access with no anonymous or publishable keys; and immediate deletion of credentials when a user disconnects a broker or deletes their account.
- **Unauthorized access to production systems or personal data.** Treatment: multi-factor authentication on administrative accounts, least privilege, and review of provider audit logs.
- **Subprocessor or provider failure or breach.** Treatment: vendor review, data processing agreements, and the restriction of what data is sent to each provider.
- **Loss of availability or data.** Treatment: provider-managed backups and recovery procedures (see the Business Continuity and Disaster Recovery Plan).

7. Risk mitigation

- When the net risk is below 3, there are reasonable grounds to deem the risk acceptable.
- For higher values, a risk may still be accepted if the cost of the mitigation measures exceeds the financial impact the risk could cause. The reasoning must be recorded in the risk register.
- If a risk cannot be mitigated and the net risk exceeds 8, Taufolio must consider transferring part of it, for example by insurance, and must use the expected financial impact to size the cover.
- Threats and risks must be ranked in descending order of net risk, which sets the order in which they are addressed. Controls are designed for the risks selected for mitigation, and a plan implements them in that order.
- After the controls and mitigation strategies are fully implemented, the residual risk is computed. Based on it, one of the following decisions is made and recorded:
 - accept the risk;
 - transfer the risk;
 - add more controls;
 - take other actions as necessary.
- When the risk assessment is complete, the results must be communicated to the affected staff members.

8. Document security classification

Public. This document is published in the Taufolio Trust Center. See the Data Classification Policy for the classification levels.

9. Non-compliance

Compliance with this policy is verified through the risk register reviews, provider audit logs, periodic internal reviews and feedback to the policy owner. Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or of their contractual agreement. The action depends on the extent, intent and consequences of the violation.

10. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for maintaining the risk register. Staff members are responsible for applying the relevant sections of this policy in their own work.

11. Schedule

This document is reviewed at least annually and whenever a significant change occurs in Taufolio's systems or organization.

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

12. Version history

Version	Change	Approved by	Date
1 (current)	Taufolio policy issued for the Taufolio service and published in the Taufolio Trust Center	Jacek Janczura, owner	18 October 2026