Enterprise Risk Assessment Framework

Aligned with ISO 31000

A Practical Application for a Financial Technology Organisation

FinSure Payments Ltd.

(Fictional Case Study)

Prepared By: Sachin Verma

Programme: MSc in Business Analytics

Academic Year: 2025-2026

Table of Contents

1. Introduction

This project presents the design and application of an Enterprise Risk Assessment Framework aligned with ISO 31000. The purpose of the project is to identify, analyse, evaluate, and treat key risks that may affect the achievement of organisational objectives. The assessment adopts a structured and risk based approach to support effective decision making, accountability, and resilience. By applying recognised risk management principles, the framework aims to enhance governance practices and provide management with clear visibility of the organisation's risk profile.

2. Organisation Overview

FinSure Payments Ltd. is a fictional mid sized financial technology company headquartered in Dublin, Ireland. The organisation provides digital payment processing services to small and medium sized enterprises as well as individual customers across Ireland and the wider European Union. Its core services include online payment gateways, digital wallets, and transaction processing platforms.

The company operates in a highly regulated and technology driven environment. It relies extensively on cloud based infrastructure, third party service providers, and digital platforms to deliver its services. As a result, the organisation is exposed to a range of strategic, operational, financial, compliance, and technology related risks. Effective enterprise risk management is therefore critical to ensuring regulatory compliance, maintaining customer trust, and supporting sustainable business growth.

3. Risk Management Framework (ISO 31000)

The enterprise risk management framework adopted for this project is aligned with the principles and process outlined in ISO 31000. The framework is designed to support a consistent and structured approach to managing risk across the organisation.

- Risk management is integrated into organisational governance and decision making processes rather than treated as a standalone activity.
- Risks are identified and assessed in the context of the organisation's strategic objectives, operating environment, and regulatory obligations.
- A structured risk assessment process is applied, including risk identification, risk analysis, risk evaluation, and risk treatment.
- Risks are assessed using a standardised likelihood and impact scoring methodology to ensure consistency and comparability.
- Existing controls are considered when determining residual risk exposure.
- Clear ownership is assigned to each identified risk to support accountability and effective management.
- Key Risk Indicators are used to support ongoing monitoring and early identification of emerging risk trends.

- The framework supports continuous monitoring and review to ensure that risks remain within the organisation's defined risk appetite and tolerance levels.

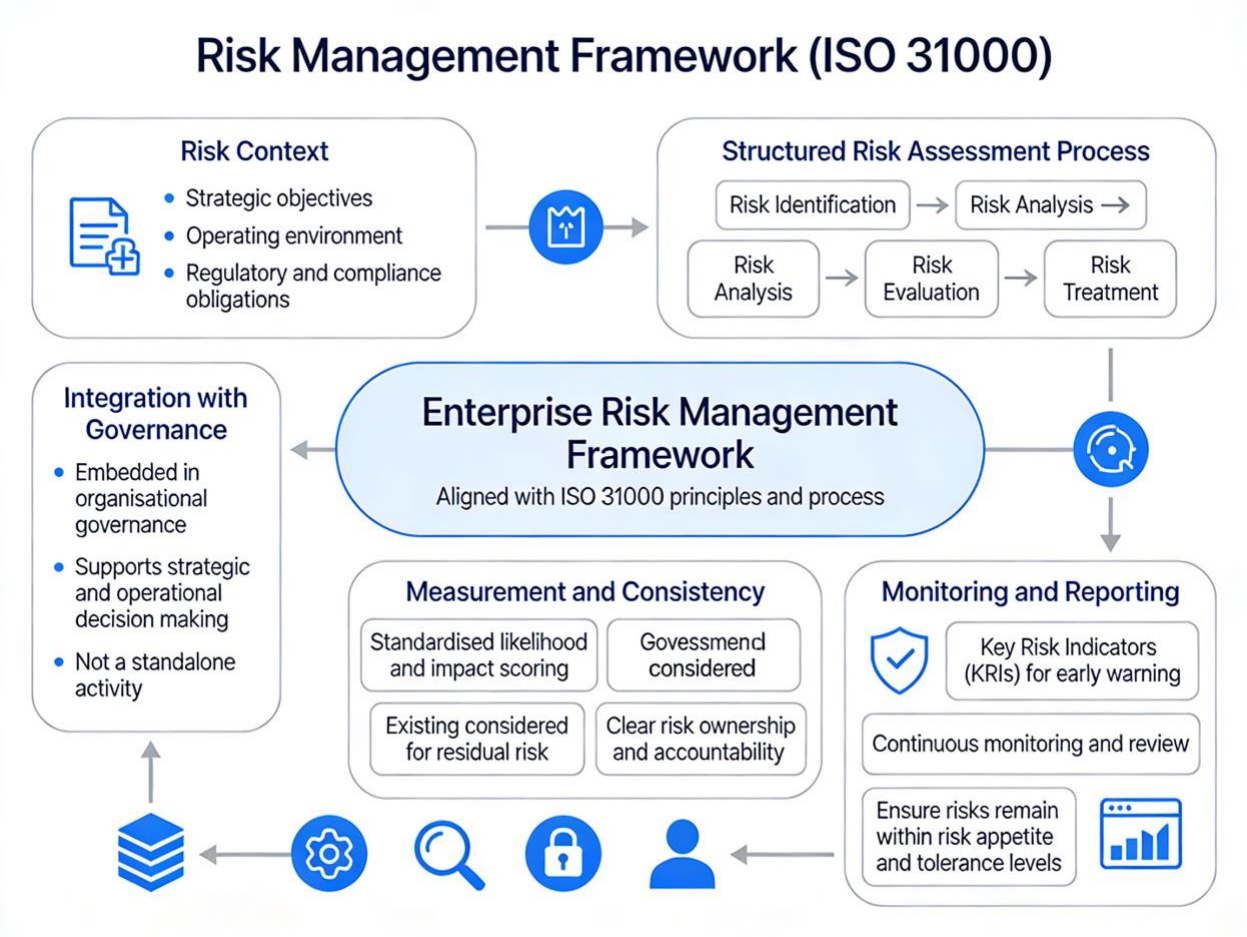

Figure 1: Enterprise Risk Management Framework aligned with ISO 31000.

4. Risk Governance and Risk Appetite

- Risk governance is established to ensure risks are managed in a consistent, structured, and accountable manner across the organisation.
- Each identified risk is assigned to a defined role, ensuring clear ownership and responsibility for oversight and management.
- Risk owners are responsible for monitoring their risks, maintaining appropriate controls, and escalating issues where required.
- Escalation procedures are applied for risks that exceed acceptable tolerance levels or require senior management attention.
- The organisation adopts a risk based approach to decision making, recognising that controlled risk taking is necessary to achieve strategic objectives.
- Risk appetite defines the level and type of risk the organisation is willing to accept in pursuit of its objectives.

- A low risk tolerance is applied to compliance, data protection, and cyber security risks due to regulatory obligations and potential impact on trust.
- A moderate risk tolerance is applied to operational and strategic risks where risks are understood and appropriately controlled.
- Risks with high residual risk ratings are prioritised for treatment and ongoing monitoring, while low risks within tolerance may be accepted.

5. Risk Identification

- Risk identification was carried out to determine events and conditions that could affect the achievement of organisational objectives.
- The approach focused on enterprise wide risks rather than isolated operational issues, in line with ISO 31000 guidance.
- Risks were identified by reviewing the organisation's business model, regulatory environment, operational dependencies, and technology landscape.
- A structured categorisation of risks was applied to support consistent assessment, ownership, and prioritisation.

6. Risk Category

Risk Category	Description	Typical Examples
Strategic Risks	Risks that may affect the organisation's long-term objectives and strategic direction.	Changes in competitive environment, regulatory landscape, or risks from strategic decision making.
Operational Risks	Risks resulting from failures in internal processes, people, or systems.	Impacts on service delivery, operational efficiency, or business continuity.
Financial Risks	Risks related to the organisation's financial performance and stability.	Revenue volatility, cost control issues, fraud, and weaknesses in financial controls.
Compliance Risks	Risks arising from failure to comply with applicable laws, regulations, and industry standards.	Data protection breaches, regulatory reporting failures, and not meeting supervisory expectations.
Cyber and Information Technology Risks	Risks affecting the confidentiality, integrity, and availability of information and systems.	Cyber attacks, system outages, and technology control weaknesses.
Reputational Risks	Risks that may damage stakeholder confidence and public trust in the organisation.	Service disruptions, regulatory breaches, or security incidents that harm the organisation's reputation.
Purpose of Categorisation	Categorising risks supports clearer analysis, accountability, and targeted risk treatment actions.	Enables focused mitigation plans, clearer ownership, and better reporting to management and stakeholders.

7. Risk Register and Risk Assessment

- The risk register acts as the central record of all identified enterprise risks and provides a consolidated view of the organisation's risk exposure.
- It captures key information for each risk, including risk description, categorisation, ownership, risk ratings, controls, and monitoring indicators.

- The risk register supports consistency in risk assessment and enables prioritisation of risks based on their potential impact on organisational objectives.
- Risk assessment is performed using a standardised scoring methodology based on likelihood and impact.
- Likelihood represents the probability of a risk occurring within the operating environment, while impact reflects the potential severity of consequences if the risk materialises.
- Both likelihood and impact are assessed using a five point scale to ensure consistency and comparability across all risks.
- Inherent risk ratings are determined before considering existing controls to reflect the organisation's initial exposure.
- Existing controls are reviewed to assess their effectiveness in reducing risk exposure.
- Residual likelihood and impact ratings are then assigned to reflect the level of risk remaining after controls are applied.
- Risks with high inherent or residual risk ratings are prioritised for further treatment and enhanced monitoring.
- Medium risks are monitored to ensure they remain within defined tolerance levels.
- Low risks within tolerance may be accepted, subject to ongoing oversight.
- Each risk is assigned to a defined role to ensure clear accountability for management and monitoring.
- Key Risk Indicators are defined for each risk to support ongoing monitoring and early identification of changes in risk exposure.
- The risk register is treated as a dynamic management tool and is reviewed periodically to reflect changes in the operating environment, regulatory requirements, and strategic objectives.

Residual risk scores are assessed against the organisation's defined risk appetite, with risks remaining above acceptable tolerance levels prioritised for further mitigation or escalation to senior management. The inherent and residual risk heat maps support this process by highlighting concentrations of higher risk, enabling management to focus attention and resources on risks with the greatest potential impact and to track the effectiveness of risk treatment actions.

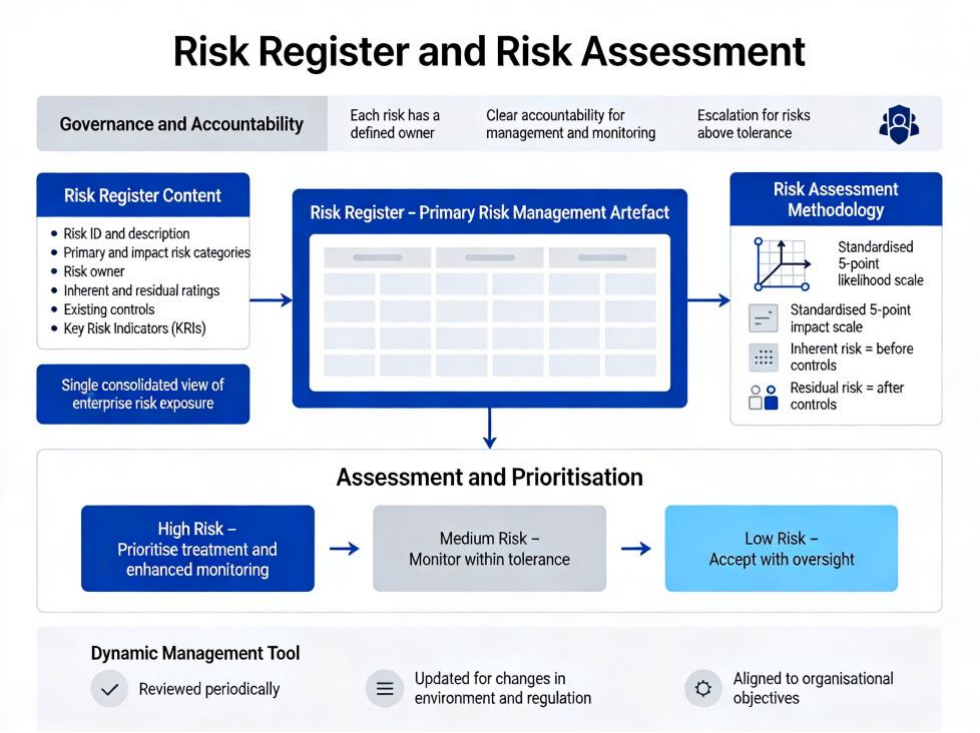

Figure 2: Integrated view of the enterprise risk register and standardised risk assessment, showing ownership, scoring, and prioritisation of risks across the organisation.

8. Inherent & Residual Risk Heat Maps

The inherent and residual risk heat maps are maintained within the risk register workbook to provide a clear visual summary of the organisation's risk profile. The inherent risk heat map illustrates the concentration of risks before the application of controls, supporting prioritisation of areas with higher potential impact and likelihood. The residual risk heat map demonstrates the effect of existing controls by showing the movement of risks to lower likelihood and impact levels. Together, these heat maps support management decision making, enable comparison of risk exposure before and after mitigation, and provide a concise view of overall risk reduction achieved through the risk management framework.

9. Risk Treatment and Control Mapping

Risk treatment actions are defined to ensure that identified risks are managed in line with the organisation's risk appetite and governance arrangements. The objective of risk treatment is to reduce risk exposure to an acceptable level through the application of appropriate controls, rather than to eliminate risk entirely. Risk treatment decisions are informed by inherent and residual risk ratings, regulatory requirements, and business priorities.

For risks assessed as high or medium, key controls have been identified and mapped to each risk to address either the likelihood of occurrence, the potential impact, or both. Controls include

preventive measures designed to reduce the probability of a risk materialising, as well as detective measures that enable timely identification and response. These controls are documented within the control register and linked directly to the relevant risks in the risk register.

Each control is assigned to a defined role to ensure clear accountability for implementation and ongoing operation. The effectiveness of controls is considered when determining residual risk ratings, and risks that remain above acceptable tolerance levels are prioritised for further mitigation or management review. Risks assessed as low and within tolerance may be accepted, subject to continued monitoring through defined key risk indicators.

This structured approach to risk treatment and control mapping supports transparency, consistency, and effective oversight. It enables management to understand how risks are mitigated in practice, identify control gaps, and ensure that risk management activities remain aligned with organisational objectives and the operating environment.

While existing controls reduce the likelihood and impact of identified risks, it is recognised that controls are not infallible and may fail or degrade over time, reinforcing the need for ongoing monitoring, testing, and review.

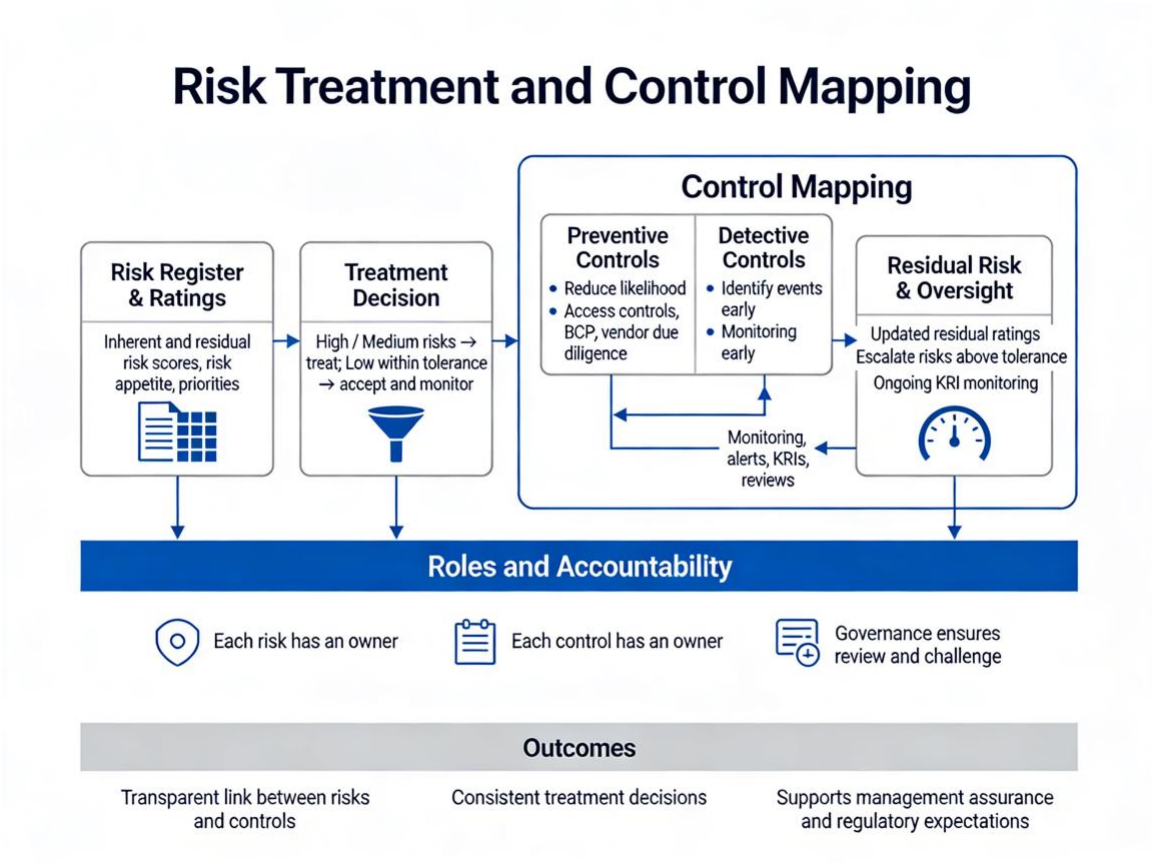

Figure 3: Risk treatment flow showing how high and medium risks are mapped to preventive and detective controls to reduce exposure to an acceptable residual level.

10. Monitoring and Review

- Monitoring and review activities are established to ensure that risks remain within acceptable tolerance levels and that controls continue to operate effectively over time.
- Ongoing monitoring supports early identification of changes in risk exposure arising from internal or external factors.
- Key Risk Indicators defined in the risk register are used as the primary mechanism for monitoring changes in risk levels.
- KRIs are reviewed on a periodic basis by risk owners to identify emerging trends, control weaknesses, or increasing risk exposure.
- Risk owners are responsible for reviewing the risks assigned to them, confirming the continued effectiveness of existing controls, and updating risk information where required.
- Any material changes to risk likelihood, impact, or control effectiveness are reflected in updates to the risk register.
- Risks with increasing residual risk ratings or breaches of defined tolerance levels are escalated in accordance with the organisation's risk governance arrangements.
- High and emerging risks identified through monitoring activities are prioritised for management review and further risk treatment where necessary.
- The risk register is reviewed periodically to ensure it remains accurate, relevant, and aligned with the organisation's operating environment, regulatory obligations, and strategic objectives.
- This review process ensures that the risk register continues to function as a dynamic management tool rather than a static record.

Figure 4: Continuous monitoring and review cycle that uses KRIs, owner reviews, and escalation to keep enterprise risks and controls within defined tolerance.

11. Conclusion and Business Impact

This project demonstrates the practical application of an Enterprise Risk Assessment Framework aligned with ISO 31000 within a regulated financial technology environment. A structured and consistent approach was applied to identify, assess, treat, and monitor risks that may affect the achievement of organisational objectives. The framework supports informed decision making and provides a clear view of the organisation's overall risk profile.

The risk register developed as part of this assessment provides a consolidated view of enterprise risks across strategic, operational, financial, compliance, cyber, reputational, asset, third party, and resilience domains. Clear assignment of risk ownership, defined controls, and measurable indicators strengthen accountability and enable effective oversight of risk exposure across the organisation.

The assessment supports management in prioritising risks based on inherent and residual risk levels, allowing resources and attention to be directed toward the most significant areas of exposure. High and medium risks are clearly identified for active management and treatment, while lower risks within defined tolerance levels may be accepted with appropriate monitoring. This structured prioritisation enhances efficiency and supports balanced risk taking.

By integrating risk treatment actions, control mapping, and ongoing monitoring, the framework enhances the organisation's ability to respond to emerging risks and operational disruptions. The inclusion of business continuity planning and third party risk considerations further strengthens organisational resilience and reduces dependency related vulnerabilities.

Overall, the Enterprise Risk Assessment Framework supports improved governance, regulatory compliance, operational stability, and protection of customer trust. The approach reflects industry standard risk management practices and provides a scalable foundation for continuous improvement in enterprise risk management.