In **GRC (Governance, Risk, and Compliance)**, when we say **risk management**, we are talking about a **broad process** of identifying, assessing, and mitigating risks that could affect the organization’s ability to meet its objectives — and this can cover **many domains**, not just one.

However, in **practical GRC work**, "risk management" often refers to **enterprise risk management (ERM)** or **IT risk management**, and it could include:

**1. Strategic Risks**

* **Example**: Entering new markets, mergers, or major partnerships.
* **Relevant to GRC?** Yes, because governance frameworks need to ensure these align with company policies and regulations.

**2. Operational Risks**

* **Example**:
  + **New Contracts** – risk in terms of financial exposure, compliance clauses, data privacy commitments.
  + **Change Management** – risk in changing IT systems, processes, or suppliers.
  + **Third-Party/Vendor Risks** – risks from outsourcing, supplier dependencies.

**3. Asset Risks**

* **Information Assets** – risk of data breaches, unauthorized access.
* **Physical Assets** – risk of theft, damage, loss.
* **Intangible Assets** – brand reputation, intellectual property.

**4. Compliance Risks**

* **Example**: Non-compliance with SOX, GDPR, HIPAA, PCI-DSS, etc.
* Can arise from **new processes, contracts, or changes** that are not reviewed for compliance impact.

**5. IT & Cybersecurity Risks**

* **Example**: Vulnerabilities, patching gaps, phishing attacks, insider threats.
* Change management is a big part here, because changes in systems can introduce new vulnerabilities.

✅ **So in GRC, “Risk Management” is not only about one thing like new contracts, assets, or change management — it’s about *all areas* where risks can emerge**, and it’s handled through a structured lifecycle:  
**Identify → Assess → Mitigate → Monitor → Report.**

**Risk Management Frameworks – Quick Overview**

**1. ISO 27005**

* **Purpose:** Information security risk management.
* **Scope:** Supports **ISO 27001** by providing a methodology to identify, assess, and treat **information security risks**.
* **Focus Areas:** Assets, threats, vulnerabilities, impacts, likelihood, treatment options.
* **Best For:** Organizations implementing or maintaining an ISMS (Information Security Management System).

**2. ISO 31000**

* **Purpose:** Enterprise risk management (ERM) principles and guidelines.
* **Scope:** Covers **all types of risk** — strategic, operational, financial, compliance, reputational.
* **Focus Areas:** Risk management integration into governance, decision-making, and culture.
* **Best For:** Creating a **company-wide risk management framework** beyond IT/security.

**3. NIST RMF (Risk Management Framework)**

* **Purpose:** Risk-based approach to managing **information system security** and compliance.
* **Scope:** Originally for US federal systems but widely used in regulated industries.
* **Process Steps:** **Categorize → Select → Implement → Assess → Authorize → Monitor** security controls.
* **Best For:** Aligning security controls with compliance requirements (e.g., FedRAMP, FISMA).

**4. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

* **Purpose:** Evaluate organizational risks from both **business and technical perspectives**.
* **Scope:** Involves stakeholders from across the business to identify **critical assets**, threats, and vulnerabilities.
* **Focus Areas:** Asset-driven, scenario-based, qualitative assessment.
* **Best For:** Organizations wanting **collaboration between technical and non-technical teams** in risk identification.

**5. FAIR (Factor Analysis of Information Risk)**

* **Purpose:** **Quantify** cyber and operational risks in **financial terms**.
* **Scope:** Uses a structured model to calculate **probability and financial impact** of loss events.
* **Focus Areas:** Risk as **Loss Event Frequency × Loss Magnitude**.
* **Best For:** Prioritizing investments by comparing ROI of risk mitigation measures.

**6. COSO ERM (Committee of Sponsoring Organizations – Enterprise Risk Management)**

* **Purpose:** Integrate **risk management into strategic decision-making** and performance management.
* **Scope:** Enterprise-level — includes governance, culture, performance, information, and reporting.
* **Focus Areas:** Aligning **risk appetite** with business objectives; embedding risk in corporate governance.
* **Best For:** Organizations needing a **strategic, board-level view of risk** and its impact on performance.

| **Framework** | **Scope** | **Primary Focus** | **Strengths** | **Limitations** | **Typical Use Cases** |
| --- | --- | --- | --- | --- | --- |
| **ISO 27005** | Information Security Risk Management | Asset-based risk assessment for ISMS | Directly supports ISO 27001; structured process for security risks | Narrow scope (only security-related risks) | ISMS implementation, security audits, compliance with ISO 27001 |
|  |  |  |  |  |  |
| **ISO 31000** | Enterprise Risk Management (All risks) | Governance, integration, decision-making | Universal, applies to all risk types; fosters organization-wide adoption | Not prescriptive — leaves methodology to the org | ERM programs, corporate governance, integrating risk into strategy |
| **NIST RMF** | Information System Security (compliance-heavy) | Security control selection, assessment, and monitoring | Detailed, control-oriented; compliance-focused | US federal-centric (can be heavy for smaller orgs) | FedRAMP, FISMA, PCI-DSS system authorization, regulated industries |
| **OCTAVE** | Organizational (Business + Technical Risks) | Critical asset identification and qualitative risk assessment | Encourages cross-functional involvement; asset-driven | Less quantitative; may be subjective | IT governance, operational security planning, business continuity |
| **FAIR** | Quantitative Cyber/Operational Risk | Financial impact & probability of loss events | Quantifies risk in money terms; supports ROI-based decisions | Requires good data quality; training needed for accuracy | Cyber risk quantification, insurance decisions, budget justification |
| **COSO ERM** | Enterprise Strategic Risk Management | Risk appetite, governance, performance integration | Board-level alignment; integrates risk with performance metrics | Strategic — may lack technical depth for IT risks | Public company governance (SOX), strategic planning, board reporting |

**Case Study –**

**“Cloud Banking Platform Risk Management”**

**Scenario:**  
A mid-sized financial institution is migrating its **core banking system** from an on-premises data center to a **cloud environment (AWS + SaaS integrations)**. The migration will involve:

* Handling **sensitive customer financial data** (PCI-DSS, GLBA applicable).
* Signing **new contracts** with cloud vendors & payment processors.
* **Change management** in IT infrastructure and operational workflows.
* Adoption of **AI-based fraud detection** (new tech, new risks).

The Board has asked the **GRC team** to manage **all types of risks** — security, operational, compliance, reputational, and strategic — using internationally recognized frameworks.

**How Each Framework Applies**

| **Framework** | **Focus Area** | **How It’s Applied in This Case** |
| --- | --- | --- |
| **ISO 27005** | **Information security risk management** (aligned to ISO 27001) | Identify and assess risks specific to information assets (customer data, transaction records, encryption keys) during migration. Apply risk treatment plans for cloud storage encryption, IAM, data backup, etc. |
| **ISO 31000** | **Enterprise-wide risk management** | Manage all categories of risk — not just information security — such as strategic risk of vendor lock-in, financial risk of project delays, operational risk of downtime, reputational risk from a breach. Integrate risk management into all decision-making. |
| **NIST RMF** | **System-level security & compliance for federal/regulated systems** | For systems handling financial data, implement NIST RMF steps: Categorize → Select → Implement → Assess → Authorize → Monitor security controls in the cloud banking platform. |
| **OCTAVE** | **Operationally Critical Threat, Asset, and Vulnerability Evaluation** | Engage business stakeholders to identify critical assets (core banking app, payment APIs) and examine threats & vulnerabilities in both business and technology domains. Useful for involving non-technical teams. |
| **FAIR** | **Quantitative cyber risk analysis** | Model and quantify cyber risks in financial terms — e.g., “Data breach due to cloud misconfiguration could cause $5M in losses with 15% annual probability” — to support Board investment decisions for security tools. |
| **COSO ERM** | **Strategic & operational risk integration** | Align risk appetite and tolerance with corporate strategy. Integrate financial, compliance, operational, and IT risk reporting into the enterprise risk register for the bank’s governance committees. |

**Possible Risk Examples in This Case**

1. **Strategic Risks** – Vendor lock-in with AWS, dependency on SaaS fraud detection vendor.
2. **Operational Risks** – Service downtime during migration, staff training gaps.
3. **Compliance Risks** – Non-adherence to PCI-DSS, GLBA, local banking regulations.
4. **Security Risks** – Cloud misconfigurations, insider threats, API vulnerabilities.
5. **Financial Risks** – Unexpected migration costs, penalties from SLA breaches.
6. **Reputational Risks** – Customer distrust after a service outage or breach.

**How They Work Together**

* **ISO 31000** + **COSO ERM** → Provide the **enterprise-level** risk management governance.
* **ISO 27005** + **NIST RMF** → Address **information security & compliance controls** for the cloud system.
* **OCTAVE** → Gather **operational/business perspective** of risks beyond pure technical aspects.
* **FAIR** → Provide **quantitative risk analysis** for prioritization and funding decisions.