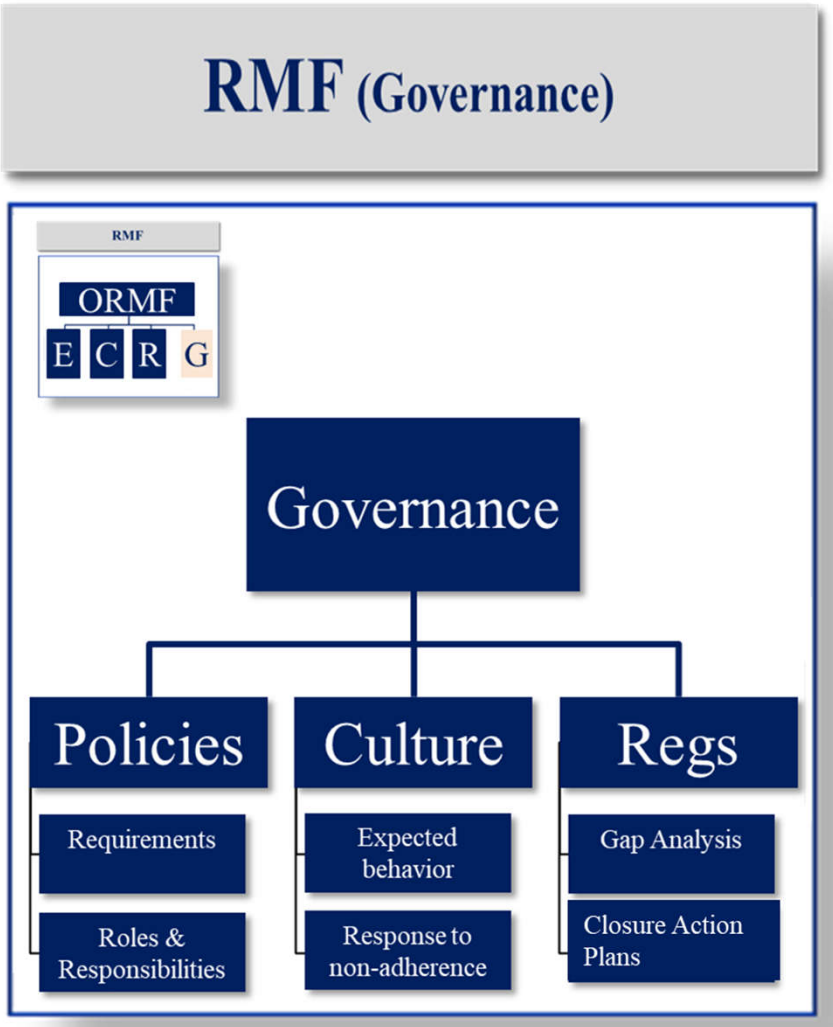
Operation Risk Management
MFRM . RSM 6304



The **Governance** structure provides guidance to effectively and efficiently implement the first three steps of the Risk Management Framework (RMF)—Exposure, Controls, and Resilience—while meeting regulatory expectations.

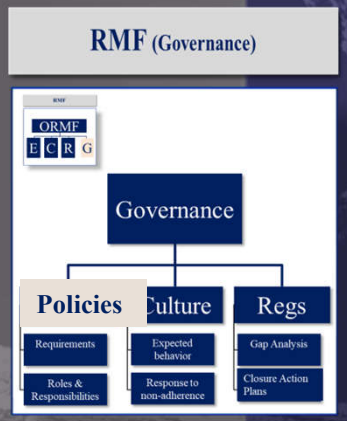
There are three components to establishing a proper governance structure:

1. Risk Management **Policies**: This includes the RMF policy and other risk management policies. These policies clearly define what needs to be done and by when (**Requirements**) and who needs to do it by when, including committees (**Roles and Responsibilities**)

2. Risk **Culture**: As a subset of corporate culture, risk culture captures the extent to which the organization has strong policies that **mandate expected behavior** and its **responses** to behavior does not adhere to policy requirements (e.g., actions taken when a trader exceeds a limit or breaches the code of conduct).

3. Risk **Regulations** are incorporated as minimum requirements in all relevant policies. A **gap analysis** is done to identify noncompliance. Where gaps exist between policies and regulatory expectations, **action plans** are developed and executed promptly to close these gaps.

Major Risk Policies



Policies

Risk Management Policies, including the RMF policy, mandate what needs to be done by when (Requirements) and who needs to do the what (Roles and Responsibilities

Operation Risk Management
MFRM . RSM 6304

- **Operational Risk Management Policy**: An overarching policy that outlines the organization's approach to identifying, assessing, managing, and monitoring operational risks. It defines the (Op) Risk Management Framework. It includes procedures for risk identification, assessment, mitigation, and reporting
- **Risk Appetite and Tolerance Policy**: Specifies the amount and type of risk the organization is willing to accept in pursuit of its objectives. It guides decision-making processes to ensure risks are managed within acceptable levels.
- **Compliance Risk Management Policy**: Ensures adherence to all relevant laws, regulations, and internal policies. It outlines procedures for compliance monitoring, reporting, and addressing non-compliance issues.
- **Information Security and Cybersecurity Policy**: Establishes guidelines for protecting the organization's information assets from cyber threats. It covers data protection, access controls, incident response, and employee training.
- **Business Continuity and Disaster Recovery Policy**: Defines plans and procedures to ensure critical business functions continue during and after a disaster or significant disruption. It includes strategies for data backup, recovery, and communication plans.
- **Third-Party Risk Management Policy**: Addresses risks associated with outsourcing and partnerships. It sets standards for due diligence, contract management, monitoring, and termination of vendor relationships.
- **Fraud Risk Management Policy**: Aims to prevent, detect, and respond to fraud within the organization. It includes measures for fraud risk assessment, internal controls, reporting mechanisms, and investigative procedures.
- **Model Risk Management Policy**: Addresses risks associated with the development, implementation, and use of models in decision-making processes. It outlines procedures for model validation, governance, and performance monitoring to ensure models are accurate, reliable, and used appropriately.
- **Change Management Policy**: Establishes procedures for managing changes to systems, processes, or organizational structures to minimize disruptions. It covers change request processes, impact analysis, testing requirements, approvals, and documentation.
- **Data Governance Policy**: Outlines how the organization manages data quality, integrity, and availability. It includes data ownership, data lifecycle management, data privacy compliance, and standards for data collection and usage.

Risk Policies Roles and Responsibilities

- **Senior management and Board of Directors**: active involvement from the board of directors and senior management in risk management practices. They should set the organization's risk appetite, approve risk policies, and integrate risk considerations into strategic decisions, as mandated by regulations such as OSFI guidelines, the Sarbanes-Oxley Act, etc.
- **First Line of Defense**: Business management, including support functions like HR, Finance, Tech and Ops, are responsible for directly managing risks and maintaining effective internal controls
- **Second line of Defense**: Independent Risk Management and Compliance Establish the RMF, monitor risk-related activities and non- compliance to the RMF and regulations, escalate risk issues as appropriate. Enables the organization to manage risk, including identifying exposures, control then to within the RA, building the resilience requirements, and the governance structure for the organization to effectively and efficiently manage its risks. Primary interface with regulators on risk related regulations.
- **Third Line of Defense**: (internal audit function), provides independent assurance on the effectiveness of governance, risk management, and internal controls.
- **Risk Committees**: Consisting of First, Second line of defenses with Third Line (IA) as an observer. Reviews and approves frameworks, policies, and procedures to identify, assess, monitor risks, resiliency capabilities and the governance structure. It reviews escalations and approves appropriate action plans. Does deep dives as need. Reviews and responds to policy exceptions, Reviews and responds to gap analysis and action plans. Approves limits and the Risk Appetite. Reviews and responds to major Financial and Reputational Loss Events, and actions from lesson learned. Reviews and responds to regulatory compliance issues. (in some institutions, regulatory compliance issues are dealt by a separate Compliance Committee) Reviews and responds to risk culture issues

Risk Policies Roles and Responsibilities

Sample RC Agenda Item	Time (Minutes)	Presenter(s)	Action Items
1. Welcome and Opening Remarks	5	Chairperson	- Call the meeting to order. - Confirm attendance and quorum. - Outline the meeting's action-focused objectives.
2. Approval of Agenda and Previous Minutes	5	Chairperson	- Review and approve the current agenda. - Approve minutes from the previous meeting. - Address any outstanding action items from prior meetings.
3. Review of Escalated Risk Issues and Approval of Action Plans	15	First and Second Line Representatives	- Present escalated risks requiring immediate action. - Review proposed mitigation strategies. - Approve action plans with responsibilities and deadlines.
4. Policy Exceptions and Decisions	10	Policy Owners	- Discuss requests for exceptions to existing risk policies. - Approve or reject exception requests. - Determine if policy amendments are necessary.
5. Gap Analysis Findings and Closure Plans	10	Compliance Officer / Risk Manager	- Summarize key gaps identified between practices and regulatory expectations. - Approve action plans to address each gap. - Assign responsibilities and timelines. - Establish monitoring mechanisms.
6. Approval of Risk Appetite Statement and Limits	15	Chief Risk Officer	- Discuss changes or updates to the risk appetite statement. - Approve quantitative limits for various risk categories.
7. Major Financial and Reputational Loss Events	15	Incident Response Team Leader	- Brief on recent significant loss events. - Approve corrective measures. - Assign ownership for implementing lessons learned.
8. Risk Culture Assessment and Actions	15	HR Director / Culture Champion	- Highlight incidents impacting risk culture. - Approve programs or training to strengthen risk culture. - Set expectations for behavior and accountability. - Approve plans to address compliance issues.
9. Any Other Business (AOB)	2	All	- Address additional urgent matters not covered in the agenda.
10. Summary of Decisions and Action Items	6	Chairperson	- Recap decisions made. - Summarize action items, responsibilities, and deadlines. - Ensure clarity on next steps.
11. Closing Remarks and Adjournment	2	Chairperson	- Confirm date and time of the next meeting. - Adjourn the meeting.

Risk Culture

Risk Culture (RC) is a subset of an organization's overall culture, and the two must be aligned. Risk culture comprises two components: the **expected behaviors** as codified in risk policies, and the **response actions** the organization takes when behavior does not comply with these expectations..

- A strong RC involves having clear and robust policies that mandate expected behaviors, as well as a strong response to any deviations from those expected behaviors.

Examples of Expected Behaviors:

- Adherence to Compliance Procedures: Employees are expected to strictly follow regulatory requirements and internal policies. For example, a risk manager should ensure that all transactions comply with anti-money laundering (AML) regulations by conducting due diligence checks.
- Proactive Risk Identification: Staff members are encouraged to actively identify and report potential risks. For instance, if an employee notices unusual login attempts in the system, they should report this immediately to the cybersecurity team.
- Ethical Conduct: Upholding ethical standards is crucial. An example is a trader who must avoid conflicts of interest by not engaging in insider trading based on non-public information.

Examples of Response Actions to Non-compliance :

- Investigation and Disciplinary Action: If an employee violates a policy, such as a trader exceeding their authorized trading limits, the organization should promptly investigate the incident and apply appropriate disciplinary measures, which could include suspension or termination.
- Reinforcement of Policies Through Training: In cases where deviations occur due to a lack of understanding, the company should provide additional training. For example, if multiple employees fail to follow data privacy protocols, organizing a refresher course on data protection can reinforce the importance of these policies.
- System and Process Improvements: Sometimes, deviations highlight weaknesses in existing systems. If employees are bypassing a cumbersome approval process, the organization might streamline the procedure to encourage compliance while maintaining control.

Risk Regulations

A key component of governance within a Risk Management Framework is meeting regulatory expectations. Organizations ensure compliance through a comprehensive structured process involving several steps:

1. **Conducting a Gap Analysis**: The organization performs a thorough review to identify all material discrepancies between its current policies and practices and the regulatory requirements. This analysis pinpoints specific areas where the organization falls short of compliance.

2. **Developing and Implementing Gap Closure Plans**: Once gaps are identified, the organization formulates detailed plans to address them. These plans outline:
    1. **Specific Actions**: What needs to be done to bridge each gap.
    2. **Assigned Responsibilities**: Who is accountable for implementing each action.
    3. **Timelines**: Deadlines by which each action should be completed.
    4. **Monitoring Progress**: The organization continuously tracks the implementation of the gap closure plans to ensure that actions are being completed on schedule.
    5. **Addressing Obstacles**: If obstacles or delays are encountered, these issues are escalated to appropriate levels of management. Remedial actions are then taken to overcome challenges and keep the compliance efforts on track.

Risk Regulations

Examples:

Example 1: Enhancing Cybersecurity Compliance

•**Gap Analysis**: A financial institution discovers that its cybersecurity measures do not fully comply with new regulatory standards for data protection and incident response.

•**Gap Closure Plan**:

- **Actions**:
  - Upgrade firewall and encryption technologies.
  - Implement multi-factor authentication for all users.
  - Develop an incident response plan.
- **Responsibilities**:
  - The IT Security Manager will oversee technology upgrades.
  - The Compliance Officer will develop the incident response plan.
- **Timelines**:
  - Technology upgrades to be completed within three months.
  - Incident response plan to be drafted within one month and implemented in two.

•**Monitoring Progress**:

- Weekly meetings are held to review the status of each action item.
- Progress reports are submitted to senior management bi-weekly.

•**Addressing Obstacles**:

- If the IT team encounters delays due to resource limitations, the issue is escalated to the CIO.
- Additional resources or outsourcing options are considered to meet the deadlines.

Risk Regulations

Examples:

Example 2: Adapting to New Financial Regulations

•**Gap Analysis**: A bank identifies that its lending practices are not aligned with recent changes in consumer protection laws.

•**Gap Closure Plan**:

- **Actions**:
  - Revise loan application procedures to include additional disclosures.
  - Train lending officers on new compliance requirements.
  - Update marketing materials to reflect compliant messaging.
- **Responsibilities**:
  - The Head of Lending Operations will revise procedures.
  - The HR Department will coordinate training sessions.
  - The Marketing Director will oversee updates to materials.
- **Timelines**:
  - Procedure revisions within one month.
  - Training completed within six weeks.
  - Marketing updates within two months.

•**Monitoring Progress**:

- A project manager is assigned to track all tasks.
- Monthly updates are provided to the compliance committee.

•**Addressing Obstacles**:

- If training sessions are delayed due to scheduling conflicts, the HR Department escalates the issue to department heads to prioritize attendance.
- If revisions to marketing materials face legal review delays, the Legal Department is consulted to expedite the process