



Risk Governance Model

A risk governance model describes the organizational structure, management oversight, roles,

responsibilities and accountabilities that support the development, implementation and maintenance. Your risk functions need broad jurisdiction to facilitate policy compliance through integration across business and technology senior management teams and through strong support from the Board of Directors, C-Suite, and Corporate Audit Committee. The risk function emphasizes integration of security responsibilities and controls as part of standard business processes, and requires clear accountability for policy compliance and execution of centralized or distributed security responsibilities. Risk outlines corporate governance at several levels that ensures awareness of and participation in risk management activities.

Governance Roles Responsibility (duties) Accountability (liabilities)

Board of Directors - Oversight of the effectiveness of the Program.

- Provide management with guidance and feedback for:
 - Central oversight and coordination
 - Areas of responsibility
 - Compliance Management
 - Risk measurement
 - Monitoring and testing
 - Reporting
 - Acceptable risk – Risk Appetite
 - Receive periodic reports
 - Approve the following written documents at least annually:
 - Risk Management Program
 - Information Security Policies
 - Risk Management Strategy
 - Review risk management summary and security posture statement two times per year to support regulatory requirements.
 - Internal Audit

CEO & President

- Provide guidance and oversight in support of BoD approved initiatives, to ensure legal compliance and to promote ethical behavior.

- Review C-Level risk incident reports.
- Review major initiatives to enhance overall corporate security, risk and compliance posture.

CIO

- Ensure the IT work plan, budget and resource plan support the Program objectives and effectively mitigate risks including security activities within the systems development methodology, application security initiatives, and infrastructure security objectives.
- Ensure the IT roles and responsibilities are properly communicated and that staff members are adequately educated.
- Review all information technology related written documents at least annually.
- Review Security Program, Policies, and Strategy annually.
- Review the results of key Program deliverables, testing and metrics.
- Support emergency actions to protect the institution and customers from loss of information or impact to stockholder value.
- Review Information Security technology-related Incidents.

CSO/CISO

- Ensure the Security and Risk budget and resource plans are in alignment with the Security Strategy and Program and business objectives.
- Support Functional Leaders in accomplishing Program objectives and integrating recommended practices into their respective departmental plans.
- Provide guidance and oversight regarding the management of the Program.
- Promote policies, standards and baselines to IT Senior Leadership.
- Review and approve key Program deliverables.
- Review monthly reports and performance metrics prior to distribution.
- Coordinate emergency actions to protect the institution and the customer from loss of information or impact to stockholder value.
- Review Information Security Incidents.
- Presents Security and Risk Testing to the Board of Directors / C-Suite and Audit Committee semi-annually.

CIRO / Director, Risk Management

- Communicate Board of Directors / C-Suite approved risk initiatives and ensures incorporation into overall technology strategy.
- Provide guidance and oversight for development of the Security Strategy.
- Ensure the Security Strategy mitigates the identified risk and integrates technology, polices procedures and training.
- Ensure centralized oversight / coordination of Program.
- Communicate and recommend risk initiatives to the Board of Directors / C-Suite.
- Review all written Security policies and procedures annually and as required.
- Review Information Security Program Policies and Strategy annually and as required.
- Review the results of key Program deliverables, testing and metrics.
- Support emergency actions to protect the institution and customers from loss of information or impact to stockholder value.
- Review Information Security Incidents.
- Review MSP/ASP/SaaS/M&A related information and assess for risk.
- Drive resiliency into business process, procedure and technology ensuring survivability during times of business stress.
- Provide oversight on disaster recovery and business continuity planning and preparation.
- Review Third Party Access requirements and assess for risk.
- Provide direct interface with Internal Audit and Corporate Compliance
- Interface with other risk management functions (Insurance, Finance, Supply Chain, Credit, Basel II, etc.)

Risk Steering Committee

- Provide forum for identifying approaches to dealing with new regulatory or legal requirements.
- Discuss potential operational impacts, risk and barriers with business leaders and stakeholders.
- Align and prioritize security initiatives.
- Review and approve policies and Program changes with corporate and business leadership.
- Ensure resources are effectively applied to accomplish the objectives of the Program.

- Ensure the Program components and results support its objectives. • Review monthly report of the Program oversight activities, results and recommendations.
- Review Information Security Incidents and corrective action.
- Review status of key initiatives and security strategy.

(This can go on and on ...)

You should develop a governance program, sound in principle, process and procedure while using industry standards as foundations. You should also look to expand into enterprise risk management establishing standard risk management functions within critical business areas such as finance, supply chain, and engineering. You may decide to look to this enterprise risk management framework both to satisfy out your internal control needs and to move toward a fuller risk management process. The underlying premise of enterprise risk management is that your company exists to provide value for your stakeholders.

You face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Value is maximized when your management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of corporate objectives. Enterprise risk management could enable your management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

