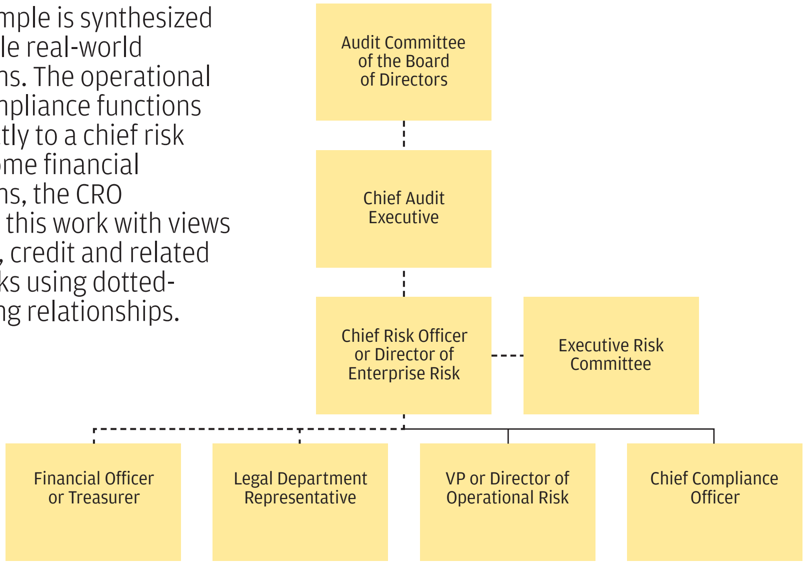
From June 2011's "ERM: Risk's Rewards"
www.csoonline.com/article/682961

Sample ERM Organizational Framework

This example is synthesized from multiple real-world organizations. The operational risk and compliance functions report directly to a chief risk officer. In some financial organizations, the CRO coordinates this work with views into market, credit and related financial risks using dotted-line reporting relationships.


Audit Committee of the Board of Directors
Chief Audit Executive
Chief Risk Officer or Director of Enterprise Risk
Executive Risk Committee
Financial Officer or Treasurer
Legal Department Representative
VP or Director of Operational Risk
Chief Compliance Officer

Specific risks can be managed by committees, which are led by the directors and officers above, working in conjunction with business unit participants.

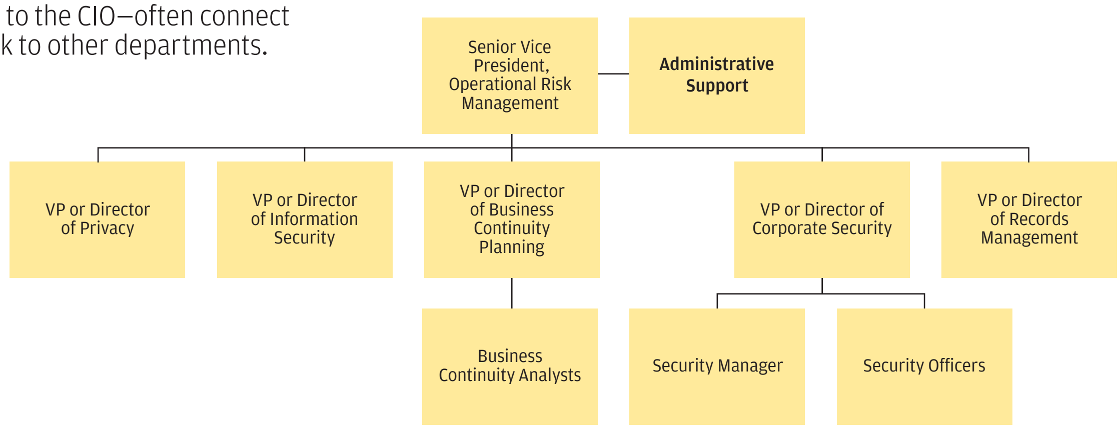
Examples of specific risks to be managed include:

- Treasury and credit functions
- Liquidity, interest rate, market and credit risks
- Legal and compliance functions
- Strategic and reputational risks and regulatory compliance
- Operational risk factors, including transactions, vendor management, IT and information security, business continuity, disaster recovery, fraud and insurance (See chart, next page.)

From June 2011's "ERM: Risk's Rewards"
www.csoonline.com/article/682961

Operational Risk Management Drill-Down

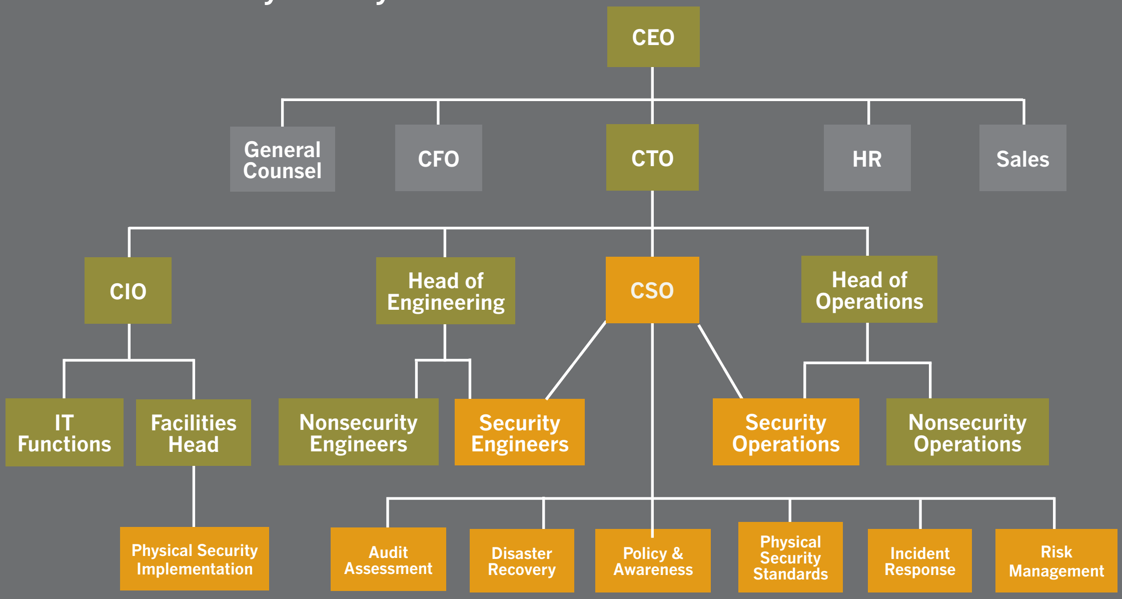
This organizational chart drills into the operational risk aspect of ERM. Dotted-line relationships—for example, from the director of information security to the CIO—often connect this work to other departments.


Senior Vice President, Operational Risk Management
Administrative Support
VP or Director of Privacy
VP or Director of Information Security
VP or Director of Business Continuity Planning
VP or Director of Corporate Security
VP or Director of Records Management
Business Continuity Analysts
Security Manager
Security Officers

For comparison: from June 2003's "All Over the Map" *www.csoonline.com/article/218166*

Responsibility Without Authority

This org chart, from a networking services company, shows how CSOs are rising in the executive ranks, without always gaining solid-line authority over key security staff.



While this CSO is responsible for setting security standards and policies—dictating building access privileges, for example—he has no direct authority to oversee the implementation of those access privileges, which instead falls to the heads of operations and facilities.

The advantage to this setup is cultural. It embeds security within the business units. The disadvantage is to the CSO, who is clearly responsible when things go wrong but has little authority to effect precautionary measures.