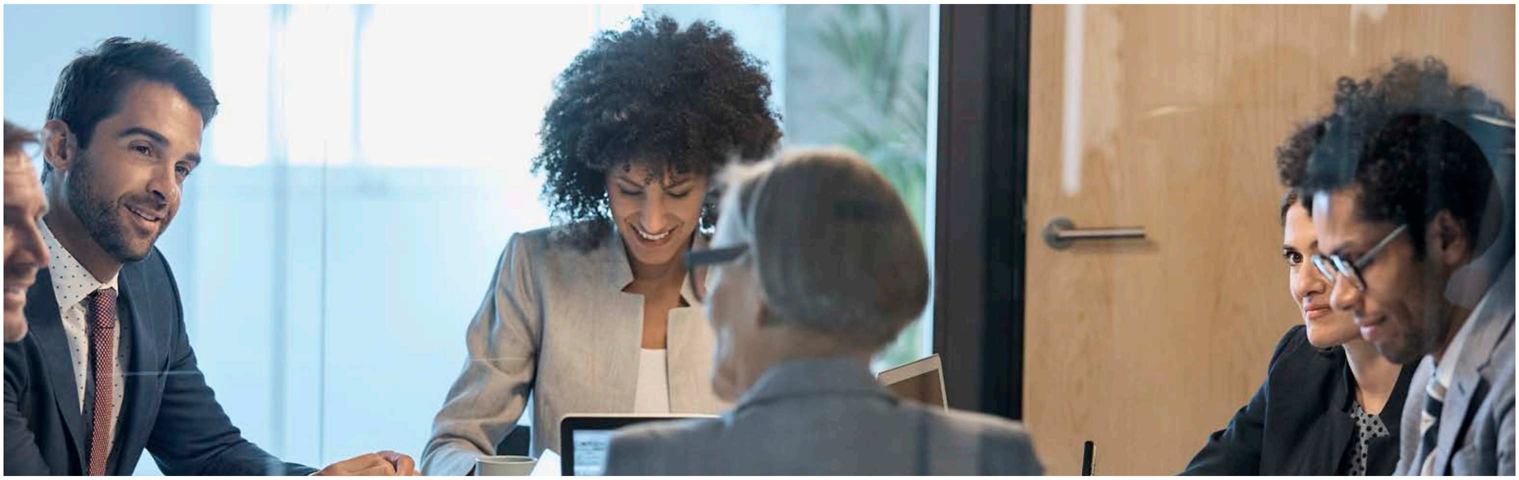
Building and Refining Enterprise Risk Management Programs, Part 1

Executives often attribute major loss incidents to isolated events driven by unprecedented factors that could not have been readily foreseen. However, a closer look into financial institutions that suffer major risk management failures often reveals risks due to systemic problems in the institution or its operating environment that could have been better identified, assessed, and controlled. Although dedicated specialists in topics such as credit risk, anti-financial crime, or treasury risk are very well adapted at spotting risk issues in their areas of focus, they are not well positioned to see the overall larger picture. An Enterprise Risk Management ("ERM") function can help illuminate the bigger picture of risk.

Risk management programs tend to be compartmentalized into specific disciplines, such as credit risk management of the lending and underwriting function, treasury analytics, and anti-financial crime risks such as Know-Your-Client/Customer ("KYC") and Anti-Money Laundering ("AML"). Organizations with more mature risk functions also have an Operational Risk team that oversees a range of risk types varying by institution, and may include risks related to transaction processing, cybersecurity, data privacy, information technology, record keeping, and other issues. Within business operating units, there are often additional specific risks that are locally understood and managed.

Sitting on top of this range of disparate risk activities is a Chief Risk Officer ("CRO") responsible for aggregating the broader view of risk and presenting it to C-suite peers and the Board of Directors.

Compartmentalized risk functions operating within a hierarchy of risk officers is a typical arrangement. Recent banking failures, however, have demonstrated that connecting the dots to fully understand the top-down view of critical risks facing the organization, and how best to go about mitigating them, can be a challenge that can lead to serious consequences if not executed properly.



Enterprise Risk Management Framework

A well-defined ERM program provides the tools, methodologies, and infrastructure to identify current and emerging risks, develop a complete risk appetite program, respond to loss incidents and near misses, and assemble a reporting package that aggregates key risk information across the enterprise into a unified and coherent view.

In addition, new and emerging risk trends such as remote work, threats and opportunities of Artificial Intelligence, and Environmental, Social and Governance mandates on the horizon, often don't have a forum to be effectively evaluated by senior management. ERM is a platform to evaluate and plan for emerging risks as well.

A class-leading ERM Framework consists of an integrated set of policies, procedures and controls that together give institutions the tools needed to establish or refine an ERM function, focusing on five integrated capabilities:

Roles and responsibilities

Robust ERM programs start with effective governance: well-defined policies and frameworks, a senior risk oversight body that provides credible review and challenge to the organization's strategic planning and execution, and controls enforcing reliable escalation of issues. Ideally, a management-level or Board-level Risk Committee ("RiskCo") will integrate the business's charter into the broader operating model. The RiskCo provides independent review and challenge of the business' strategic planning and execution processes, aggregating all forms of risk into one coherent challenge process, and instills a culture of risk management with the right "tone at the top." Risk policies approved by the RiskCo then set out roles and responsibilities at all levels of the Risk function.

Risk identification and risk inventory development

Risk identification ("Risk ID") is a foundational component of the ERM program. It describes a systemic process to workshop, understand and evaluate "inherent" and "residual" risks (the latter being the risk remaining after controls are implemented) facing the organization. The process often starts with a taxonomy of broad risks relevant to the organization and identifies a subset of risks from that taxonomy relevant to the business. The range of controls related to that risk is evaluated, and the history of events in the identified risk is considered.

Risk appetite statement development and calibration

Each revenue-generating area should generate a Risk Appetite Statement ("RAS") following a standard template to articulate in detailed terms the risks it is willing to take to meet its annual financial plan and any other requirements expected of it. Outcomes from Risk ID at the business unit level are used to structure the RAS for that business unit. The centerpiece of the RAS are calibrated limits and triggers that govern the interplay between the risk management function and the business unit's management. If real events demonstrate the business has been operating beyond its risk appetite, there should be provisions for immediate remediation.

Incident reporting and response

Logging of loss events, risk control failures, and "near misses" already exist in many institutions but are often not adequately integrated into the ERM program. Relevant controls are evaluated and can often be refined. Fact-finding often arises in incident post-mortems that can provide a valuable feedback loop into Risk ID, Risk Appetite Statements, and RiskCo reporting. The right policies and procedures ensure a complete protocol is followed in evaluating material events.

Risk aggregation and reporting

The essence of ERM is an aggregation of risks across all business areas and all risk types into a view that makes sense to all members of senior management and the Board in a brief, coherent, top-down view. The RiskCo designs a recurring reporting package that becomes an organizing tool and the medium of communication both up and across the organization. The risk inventory produced in Risk ID is a core structural tool for the reporting package. A wide range of management information is added and tailored to the scope and character of material risks, both current and emerging. A key element of RiskCo reporting is a view into the top risks facing the organization tied to transformation program activities to remediate the longer-term and more complex problems.

Building an effective ERM program requires each of these five integrated capabilities to be fully developed, tested and consistently updated to reflect changing business conditions and priorities. A successful implementation can provide senior control functions with clear consensus across the enterprise on the key risks, how they are evolving, how compliance efforts fit into the broader trajectory of risk management maturation, and whether mitigation and transformation efforts in the risk management space are effective.

For more information about building a better ERM program, read Part 2 here.

JACO SADIE
Senior Managing Director
+1 415 283 4230
jaco.sadie@fticonsulting.com

ENRIQUE UBARRI
Senior Managing Director
+1 787 910 0000
enrique.ubarri@fticonsulting.com

JANET HALE
Senior Managing Director
+1 216 403 5961
janet.hale@fticonsulting.com

PAUL FELDMAN
Senior Director
+1 212 499 3687
paul.feldman@fticonsulting.com

ANTHONY PRIMIANO
Senior Managing Director
+1 212 841 9385
anthony.primiano@fticonsulting.com

DAN HUNTER
Senior Managing Director
+1 212 499 3667
dan.hunter@fticonsulting.com