What Are the GRC Management Challenges? Enterprise-Wide Responsibility

CFO / VP Finance

- Timely notification of control issues, material weaknesses and violations
- Accurate and comprehensive information on financial exposure, compliance and audit.

Chief Compliance Officer (CCO)

- Reducing regulatory actions by reducing compliance violations
- Planning and oversight of compliance management resources
- Identifying and implementing optimal detective & preventative controls

Chief Risk Officer (CRO)

- Evaluating business requirements and technical risk capabilities
- Reducing organizational cost of risk exposure and cost of mitigation or acceptance

CIO

- Automating GRC information risk management
- Eliminating multiple internal GRC solutions
- Implementing IT platform for GRC standardisation, simplification & security

What Are the GRC Management Challenges?
Enterprise-Wide Responsibility

	CFO / VP Finance	Chief Compliance Officer (CCO)	Chief Risk Officer (CRO)	CIO
CEO	• Reducing the total cost of GRC	• Increasing efficiency & consistency of compliance processes	• Balancing the range of enterprise risks	• Ensuring Auditable secure information
	• Timely notification of control issues, material weaknesses and violations • Accurate and comprehensive information on financial exposure, compliance and audit.	• Reducing regulatory actions by reducing compliance violations • Planning and oversight of compliance management resources • Identifying and implementing optimal detective & preventative controls	• Evaluating business requirements and technical risk capabilities • Reducing organizational cost of risk exposure and cost of mitigation or acceptance	• Automating GRC information risk management • Eliminating multiple internal GRC solutions • Implementing IT platform for GRC standardisation, simplification & security

GRC - What are the objectives?

- **Governance**
  - Ultimately, Governance determines what the Board is responsible for and to what degree it entrusts day-to-day administration to the CEO, the management team and perhaps below.
- **Knowledge Management**
  - In creating a shared governance, risk and compliance environment, software supports performance objectives by regulation, standards and policy to whatever degree the Board wants.
- **Process**
  - Crucially, software enables linkage of roles, processes and assets. Plan, Do, Check. Act (PDCA) processes should be effectively managed in a single framework, so the organization as a whole is better governed
- **Technology**
  - Convergence of data, status, actions and incidents must be easily monitored, providing visibility and control to the business.

Today’s organizations are concerned about:

- Risk Management
- Governance
- Control
- Assurance

Enterprise Risk Management

PROTECT

"How Do I Reduce Business Risk?"

- Risk Analysis
- Risk Assessment
- Business Continuity Planning
- Business Resilience

OPTIMIZE

"Is my current Risk level in control?"

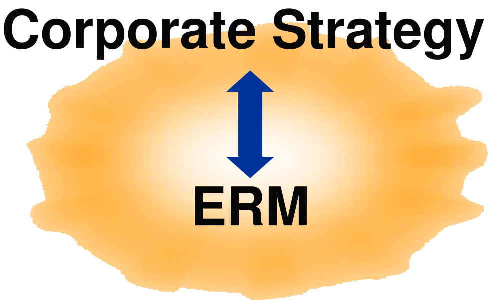
- Business Risk Monitoring
- Risk Responsiveness
- Tolerance
  - Controllable Risks
  - Non-Controllable Risks

GROW

"How Do I take more Intelligent Risks ?"

- Disciplined Decision Making
- Risk Timing
- Business & Technology Innovation
- Increased Shareholder Value
- Industry Leadership

Protect
Optimize
Grow



Primary Drivers for Implementing ERM

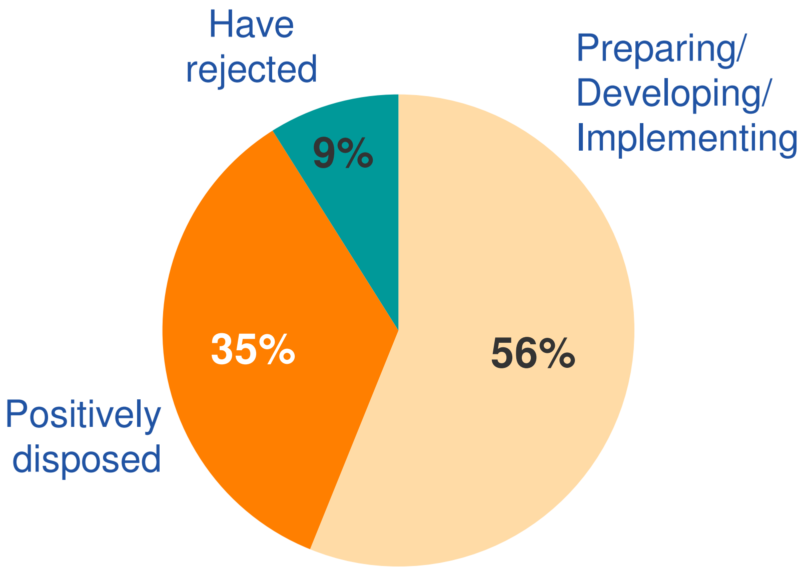
Rank	Driver	Percent
1	Corporate governance requirements	66%
2	Greater understanding of strategic and operating risks	60
3	Regulatory pressures	53
4	Board request	51
5	Competitive advantage	41

Highest Priority ERM Objectives

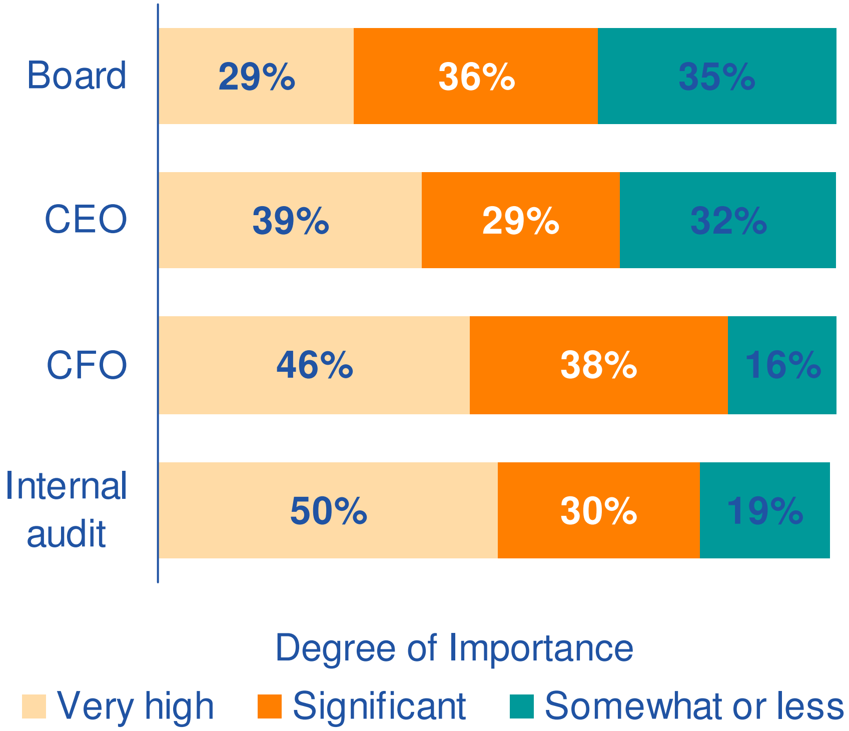
Ensure risk issues are explicitly considered in decision making	44%
Avoid surprises and “predictable” failures	40
Align risk exposures and mitigation programs	24
Institute more rigorous risk measurement	19
Integrate ERM into other corporate practices like strategic planning	17

The Growing Influence of Risk Management

A majority of companies are choosing ERM…



…and ERM is seen as an increasingly important responsibility



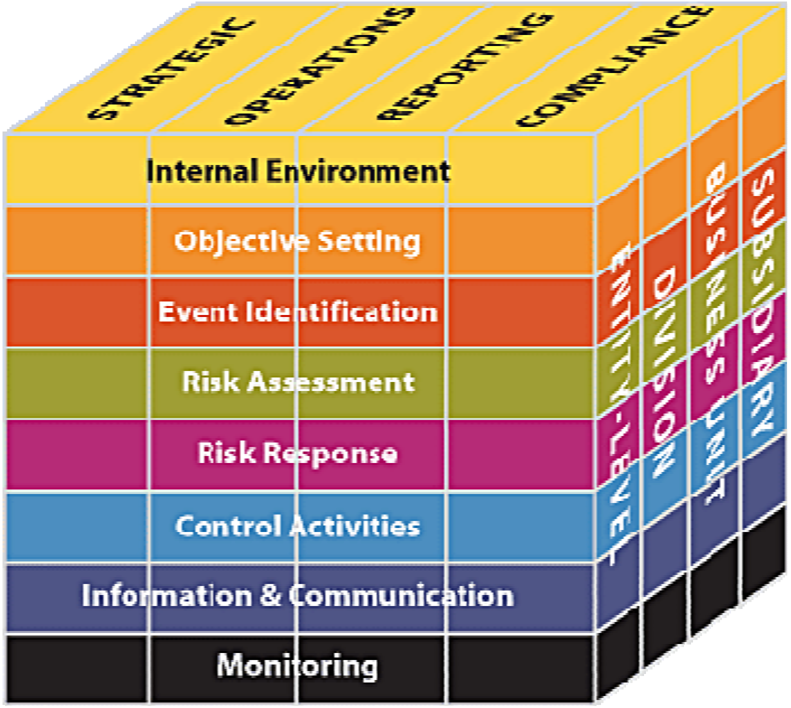
Enterprise Risk Management — An Integrated Framework

An ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

The ERM Framework

- Entity objectives can be viewed in the
- context of four categories:

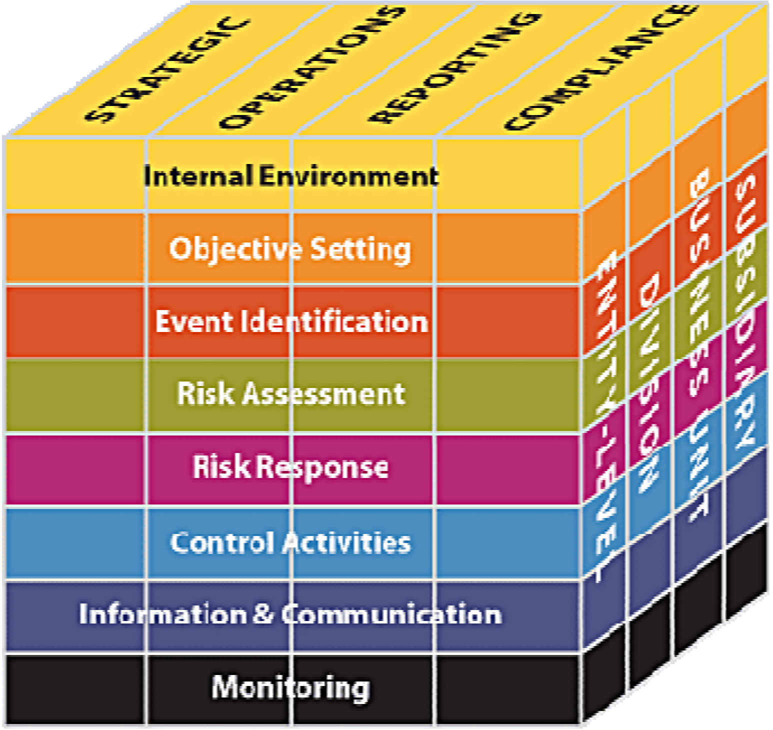
  - Strategic
  - Operations
  - Reporting
  - Compliance



The ERM Framework

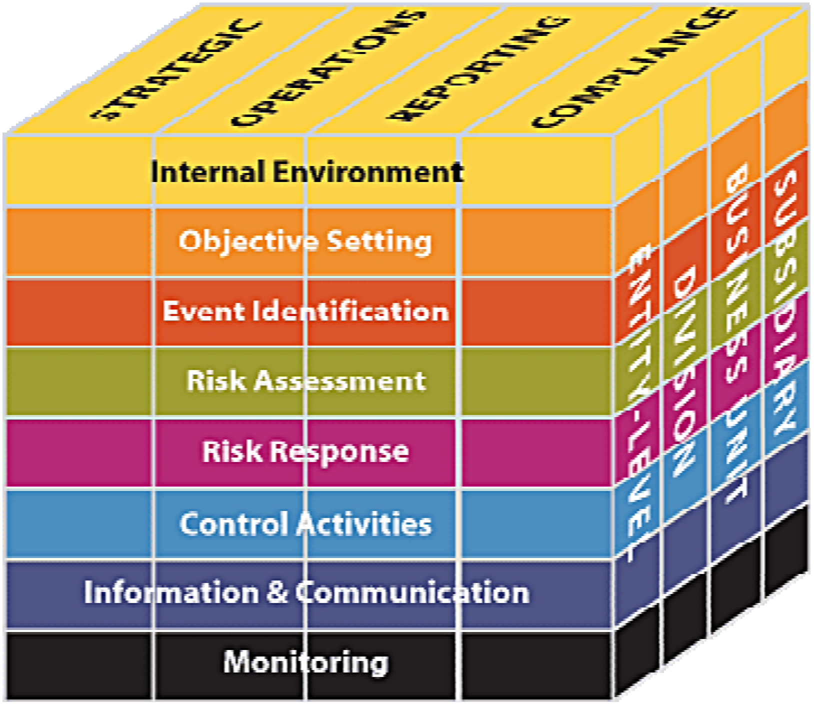
ERM considers activities at all levels of the organization:

- ♦ Enterprise-level
- ♦ Division or subsidiary
- ♦ Business unit processes



The ERM Framework

The eight components
of the framework
are interrelated …



ERM Roles & Responsibilities

- ♦ Management
- The board of directors
- Risk officers
- Internal auditors

Key Implementation Factors

1. Organizational design of business
2. Establishing an ERM organization
3. Performing risk assessments
4. Determining overall risk appetite
5. Identifying risk responses
6. Communication of risk results
7. Monitoring
8. Oversight & periodic review by management

Getting glasses: how GRC software platforms help organizations regain control

- Frequently, individuals or departments get bogged down in one area of compliance, such as Sarbanes-Oxley (SOX) or privacy laws, but fail to realize that compliance is an octopus-like challenge. Managing this many-tentacled beast requires that an organization ***establish a technology architecture for Governance, Risk, and Compliance (GRC).***
- What is the value of the GRC software platform?
  - The GRC software platform enables an enterprise risk and compliance strategy; the software is not a strategy itself. GRC software platforms must be:
    - Sustainable
    - Consistent
    - Efficient

What is a GRC software platform and what does it do ?

- The GRC software platform is the technology heart of the GRC architecture — it provides a single system of record for defining, maintaining, and monitoring Governance, Risk and Compliance. GRC platforms create centralized systems of record for the entire business in four areas:

  1. Policy, procedure, and control documentation maintenance and communication
  2. Risk and control assessment processes
  3. Risk analytics, modeling, and reporting
  4. Loss, event collection, and investigations management.

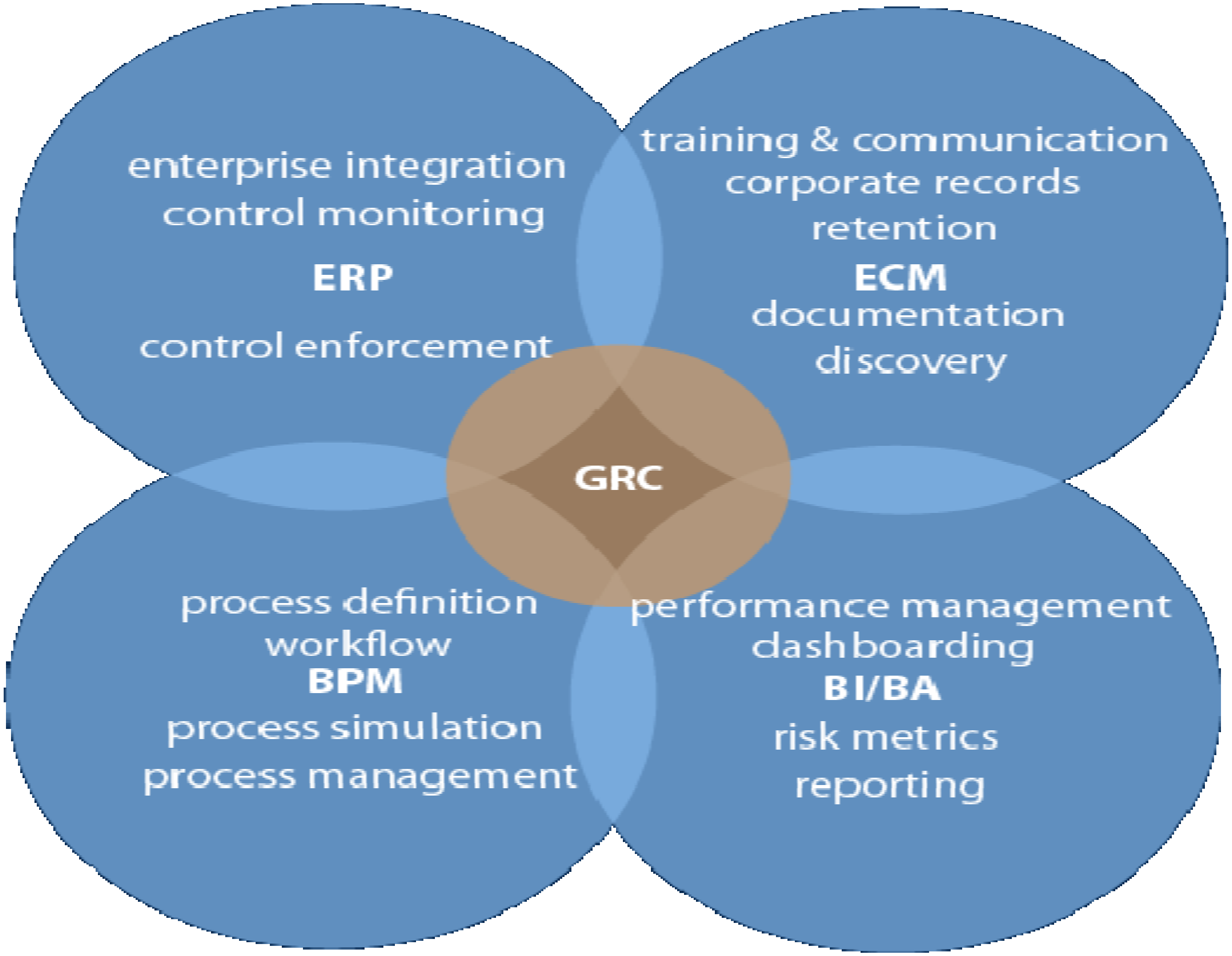
Usage varies across:

- **Business executives.** Executives use the software to monitor the state of risk and compliance, as well as to monitor corporate losses — driving strategic decisions and management of the organization.
- **Risk and compliance officers/managers.** These executives typically represent the heaviest users of the software and are focused on the day-to-day management of risk and compliance content and processes.
- **Business unit and process managers.** These executives must use the software to answer risk and control assessments and monitor the state of risk and compliance to individual areas of responsibilities.
- **Employees, contractors, consultants, and temporary workers.** The system helps every member of the firm read, acknowledge, and receive training on policies and compliance issues that pertain to their individual responsibilities.
- **Business partners.** Business partners (e.g., suppliers, contractors, outsourcers) work with the system in conducting contract and control assessments to attest to their performance to contractual requirements.

The technical support GRC software platforms need to succeed

- Achieving integration across the four capability areas that is considered essential for governance, risk, and compliance software platforms — policies/controls, assessment, analytics, and loss/investigations — requires that GRC software platforms have four integrated areas of technical functionality to deliver on these features
- **Enterprise content management.** GRC starts as a content problem. As organizations struggle to manage an assortment of risk assessment and compliance examination documentation, organizations first look for content management capabilities to categorize, store, retain, and manage access to this sensitive information.
- **Business process management.** After gaining control of content, organizations then look to drive efficiency into their GRC processes through process management and workflow technologies. Specifically, they require a platform that provides collaboration and automation of risk and compliance processes.
- **Enterprise applications.** Next, organizations look for further automation of control monitoring and enforcement alongside the monitoring and measurement of risk by gathering information directly from enterprise applications.
- **Business intelligence/business analytics.** Finally, after solving the content, process, and enterprise integration challenges of risk and compliance comes the reporting and communication requirements delivered through business intelligence and analytic features.

GRC software platforms — four capability areas



enterprise integration
control monitoring
ERP
control enforcement

training & communication
corporate records
retention
ECM
documentation
discovery

GRC

process definition
workflow
BPM
process simulation
process management

performance management
dashboarding
BI/BA
risk metrics
reporting

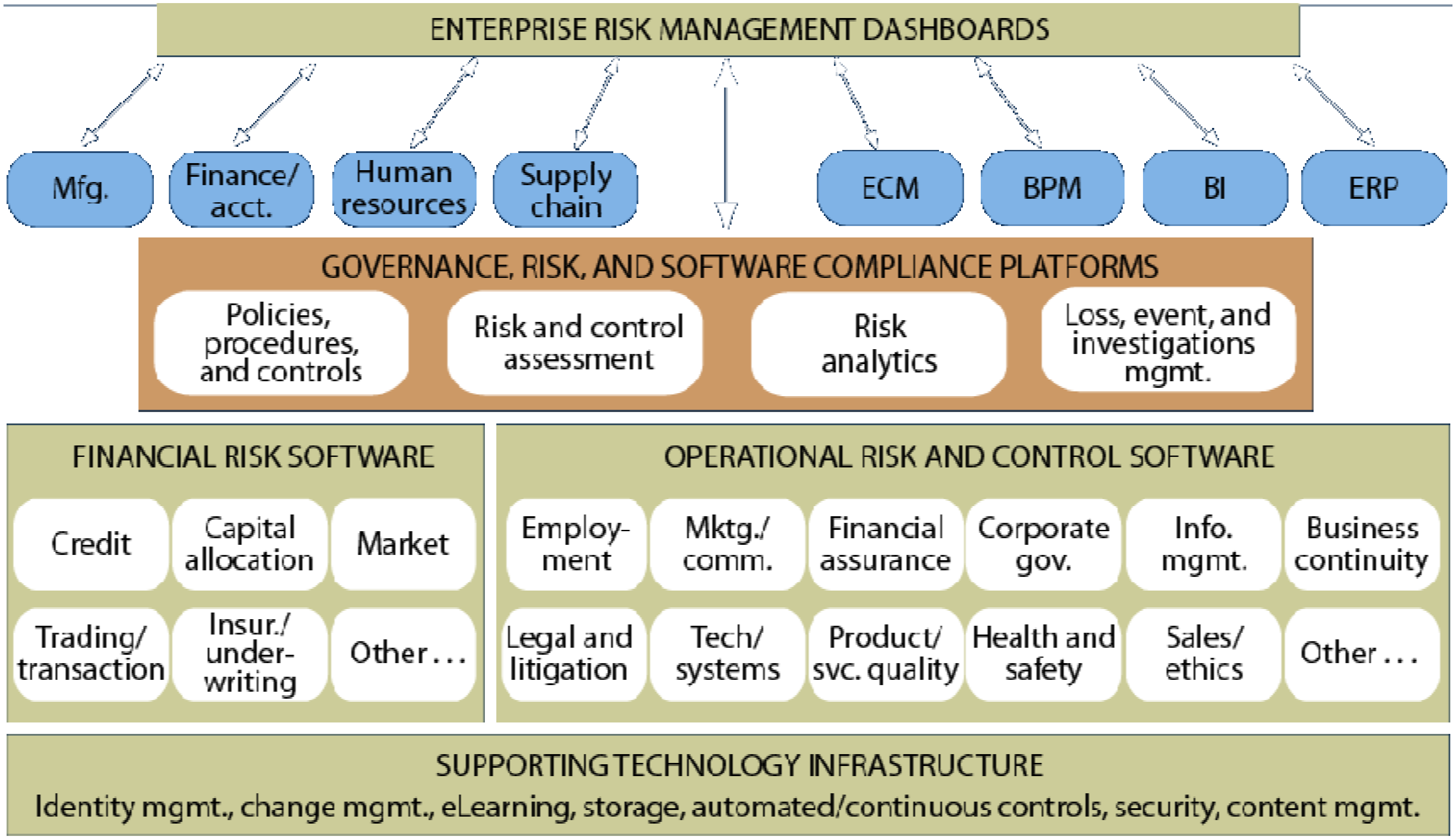
Recommendations

- Define your risk and compliance architecture.
  - A GRC software platform is not a silver bullet to manage risk and compliance — no technology is.
    - Start with defining your GRC vision.
    - Develop your long-term strategy for GRC.
    - Be selective in the platform you choose.
    - Get your feet wet first ! ! !

Common Pitfalls

- Unclear or ‘moving goalpost’ objectives
- Different ‘agendas’
- Too much detail to analyse
- Too much effort or insufficient knowledge
- Insufficient resource, takes too much time
- Answers lead to more questions
- Can’t articulate benefits to the business

Risk and compliance landscape


ENTERPRISE RISK MANAGEMENT DASHBOARDS
Mfg.
Finance/ acct.
Human resources
Supply chain
ECM
BPM
BI
ERP
GOVERNANCE, RISK, AND SOFTWARE COMPLIANCE PLATFORMS
Policies, procedures, and controls
Risk and control assessment
Risk analytics
Loss, event, and investigations mgmt.
FINANCIAL RISK SOFTWARE
Credit
Capital allocation
Market
Trading/ transaction
Insur./ under-writing
Other . . .
OPERATIONAL RISK AND CONTROL SOFTWARE
Employ-ment
Mktg./ comm.
Financial assurance
Corporate gov.
Info. mgmt.
Business continuity
Legal and litigation
Tech/ systems
Product/ svc. quality
Health and safety
Sales/ ethics
Other . . .
SUPPORTING TECHNOLOGY INFRASTRUCTURE
Identity mgmt., change mgmt., eLearning, storage, automated/continuous controls, security, content mgmt.

Thank You