Business Continuity Management and ERM

Partnership for Emergency Planning – Kansas City

Marshall Toburen
GRC Strategist – ERM, ORM, 3PM
RSA | A division of EMC^2

June 18, 2014

© Copyright 2014 EMC Corporation. All rights reserved.

Agenda

- Intro
- State of ERM Today
- ERM Universe & Risk Management Framework
- Risk Management Activities
- What it takes to Implement ERM
- Advantages/Disads of being Integrated
- Enhancing BIA, Additional Value to ERM
- Summary

© Copyright 2014 EMC Corporation. All rights reserved.

ERM Defined

*"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to **identify potential events** that may affect the entity, and **manage risk** to be within its risk appetite, to provide reasonable assurance regarding the **achievement of entity objectives**."*

Source: COSO Enterprise Risk Management – Integrated Framework, 2004.

© Copyright 2014 EMC Corporation. All rights reserved.

State of ERM Today

ERM has reached "critical mass…the point in time within the adoption curve that the sheer number of adopters assures that continued adoption…becomes self-sustaining and creates further growth."

Source: <u>2013 Enterprise Risk Management Survey</u>, RIMS-Advisen

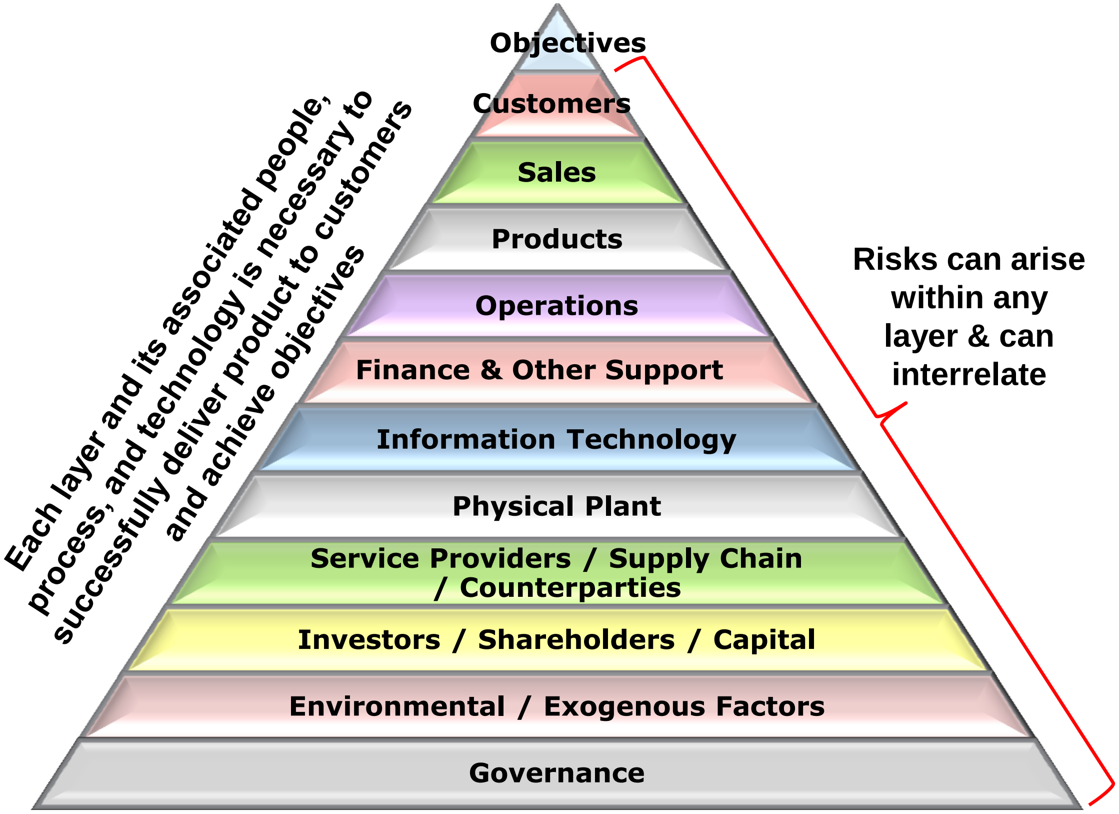
© Copyright 2014 EMC Corporation. All rights reserved.

Why ERM Acceptance Growing

- ERM tends to be viewed as strategy-focused
- Not just bad things but opportunity cost
- “Efficient frontier” orientation
  - Risk Calibration
  - Consistency in risk management
  - Balanced resource allocation
  - Performance optimization
- Stakeholder assurance of program effectiveness (including regulators)

© Copyright 2014 EMC Corporation. All rights reserved.

The ERM Universe



Objectives

Customers

Sales

Products

Operations

Finance & Other Support

Information Technology

Physical Plant

Service Providers / Supply Chain / Counterparties

Investors / Shareholders / Capital

Environmental / Exogenous Factors

Governance

Each layer and its associated people, process, and technology is necessary to successfully deliver product to customers and achieve objectives

Risks can arise within any layer & can interrelate

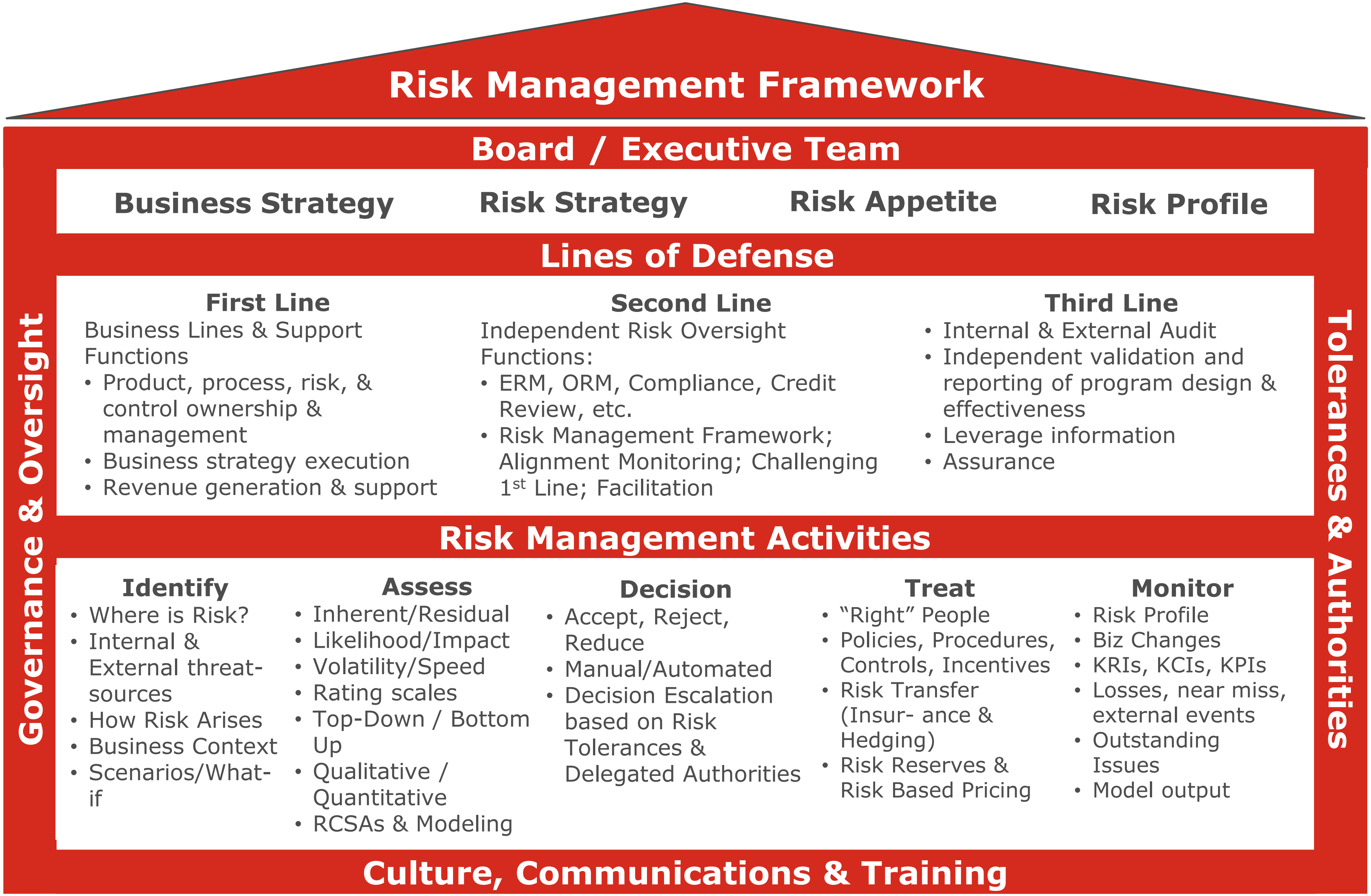
Governance is the management of these activities and the associated people, process and technologies to maximize objectives within constraints set by Management, the Board of Directors, and Regulators

ERM Presents a Diversity of Risks

(Examples)

- Human errors
- Internal or external fraud
- Information security breaches
- Disaster / business Interruption
- Violations of law & regulation
- Product liability claims
- Employee injuries
- Employee litigation claims
- Supply chain interruption
- Third-party non-performance, error, fraud
- Property damage
- Customer / counterparty credit default
- Inability to effectively market product
- Manufacturing defects
- Poorly designed processes & technologies
- Failed M&A integration
- Insufficient liquidity to fund operations
- Inadequate capital / inability to raise capital
- Political risk domestic & foreign
- Terrorism, civil unrest, war
- Inadequate liquidity
- Environmental damage
- Attracting / retaining qualified employees
- Competition
- Foreign currency fluctuation
- Income deterioration from interest rate changes
- Deterioration in investment values
- Inflation
- Sub-optimal execution

© Copyright 2014 EMC Corporation. All rights reserved.



Risk Management Framework

Board / Executive Team

Business Strategy | Risk Strategy | Risk Appetite | Risk Profile

Lines of Defense

First Line

Business Lines & Support Functions

- Product, process, risk, & control ownership & management
- Business strategy execution
- Revenue generation & support

Second Line

Independent Risk Oversight Functions:

- ERM, ORM, Compliance, Credit Review, etc.
- Risk Management Framework; Alignment Monitoring; Challenging 1st Line; Facilitation

Third Line

- Internal & External Audit
- Independent validation and reporting of program design & effectiveness
- Leverage information
- Assurance

Risk Management Activities

Identify

- Where is Risk?
- Internal & External threat-sources
- How Risk Arises
- Business Context
- Scenarios/What-if

Assess

- Inherent/Residual
- Likelihood/Impact
- Volatility/Speed
- Rating scales
- Top-Down / Bottom Up
- Qualitative / Quantitative
- RCSAs & Modeling

Decision

- Accept, Reject, Reduce
- Manual/Automated
- Decision Escalation based on Risk Tolerances & Delegated Authorities

Treat

- "Right" People
- Policies, Procedures, Controls, Incentives
- Risk Transfer (Insur- ance & Hedging)
- Risk Reserves & Risk Based Pricing

Monitor

- Risk Profile
- Biz Changes
- KRIs, KCIs, KPIs
- Losses, near miss, external events
- Outstanding Issues
- Model output

Culture, Communications & Training

Governance & Oversight

Tolerances & Authorities

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Identification

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Identification (for OpsRisk)

- Scenario Analysis.
    - Built From:
        - Practitioner experience
        - Standards
        - Incidents & Loss Events
        - Regulators, Auditors, Consultants
- pRCSAs
- Workshops vs. on-line

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Assessment

© Copyright 2014 EMC Corporation. All rights reserved.

Considerations

- Likelihood & Impact
- Inherent vs. Residual Risk
- Volatility
- Risk Categories
- Qualitative, Monetary, Stochastic
- Visual Representation of risk

© Copyright 2014 EMC Corporation. All rights reserved.

Qualitative Assessment

- High, Medium, Low – 1 through 5
- Advantages
  - Simple
  - Fast
- Disadvantages
  - Vague results
  - Disagreements over what is H, M, L
  - Difficult to Aggregate
  - Requires non-precise written definition of scale, with examples

© Copyright 2014 EMC Corporation. All rights reserved.

Monetary

- Currency Values
- Advantages
  - More meaningful to senior management and BOD
  - Easer to make Risk vs. Risk Treatment decisions
  - Better supports Risk based Capital Allocation
  - Good stepping stone to Monte Carlo
- Disadvantages
  - Disagreements over inherent risk values
  - Must translate to H, M, L and visual representation

© Copyright 2014 EMC Corporation. All rights reserved.

Monte Carlo Simulation

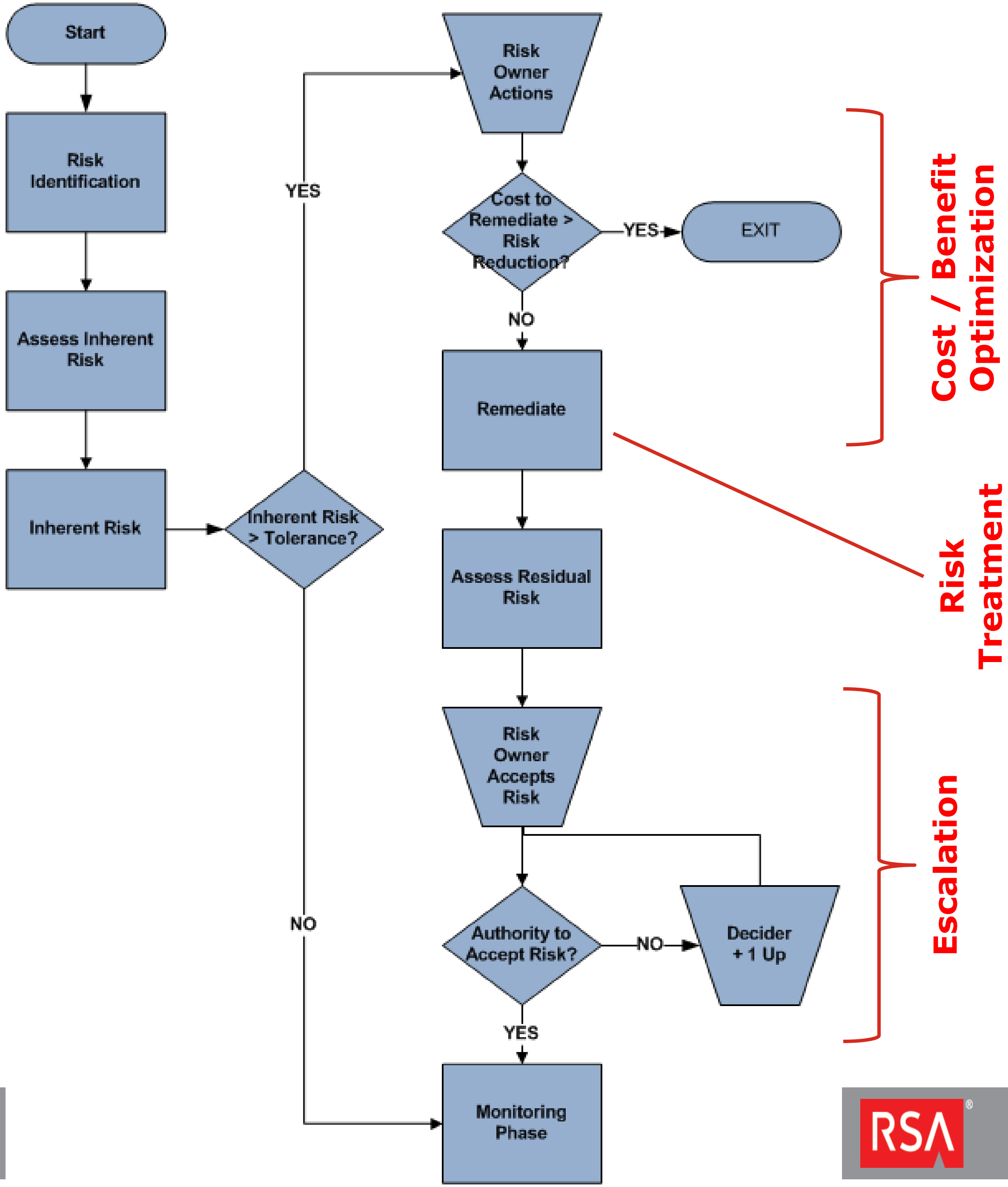
- Stochastic method that utilizes expert elicitation or loss events to estimate
- Advantages
  - More precise estimates of risk in monetary terms
    - Provides basis for capital allocation
    - Helps select appropriate limits for insurance.
  - Disadvantages
    - Can produce large numbers and management skepticism
    - Requires stochastic engine & someone that understands it somewhat

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Decisions

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Management Process Flow



© Copyright 2014 EMC Corporation. All rights reserved.

Risk Treatment

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Treatments

- Traditional Internal Controls
- Contract Risk Transfer
- Insurance Risk Transfer
- Financial Instruments (derivative hedging)

© Copyright 2014 EMC Corporation. All rights reserved.

Risk Monitoring – ERM View

© Copyright 2014 EMC Corporation. All rights reserved.

Monitoring Elements

- Loss Events (internal, external, near misses)
- Metrics (KRI, KCI, KPI)
- Internal & Regulatory Audit Findings & Remediation
- Automatic Notifications
- Reports & Dashboards

© Copyright 2014 EMC Corporation. All rights reserved.

ERM Top-down View

Enterprise-Wide *(Risk by Risk Category)*

Credit Risk	Financial Risk	Liquidity Risk	Market Risk	Operational Risk	Reputation Risk	Strategic Risk
⬆	⬇	⬇	🔴	⬆	🟠	⬆

Enterprise-Wide Operational Risk Heat Map

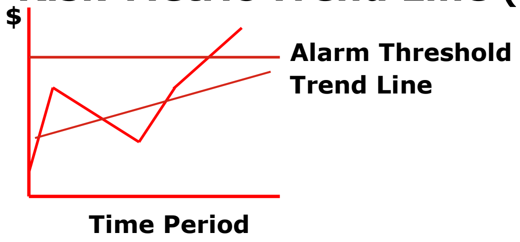
Risk Factor	Inherent Risk	Residual Risk
Information security breach	⬆	⬆
Unable to provide product & services due to disaster	🟠	🟠

Drill Down to Identify Root Cause

Division or LoB Operational Risk Heat Map

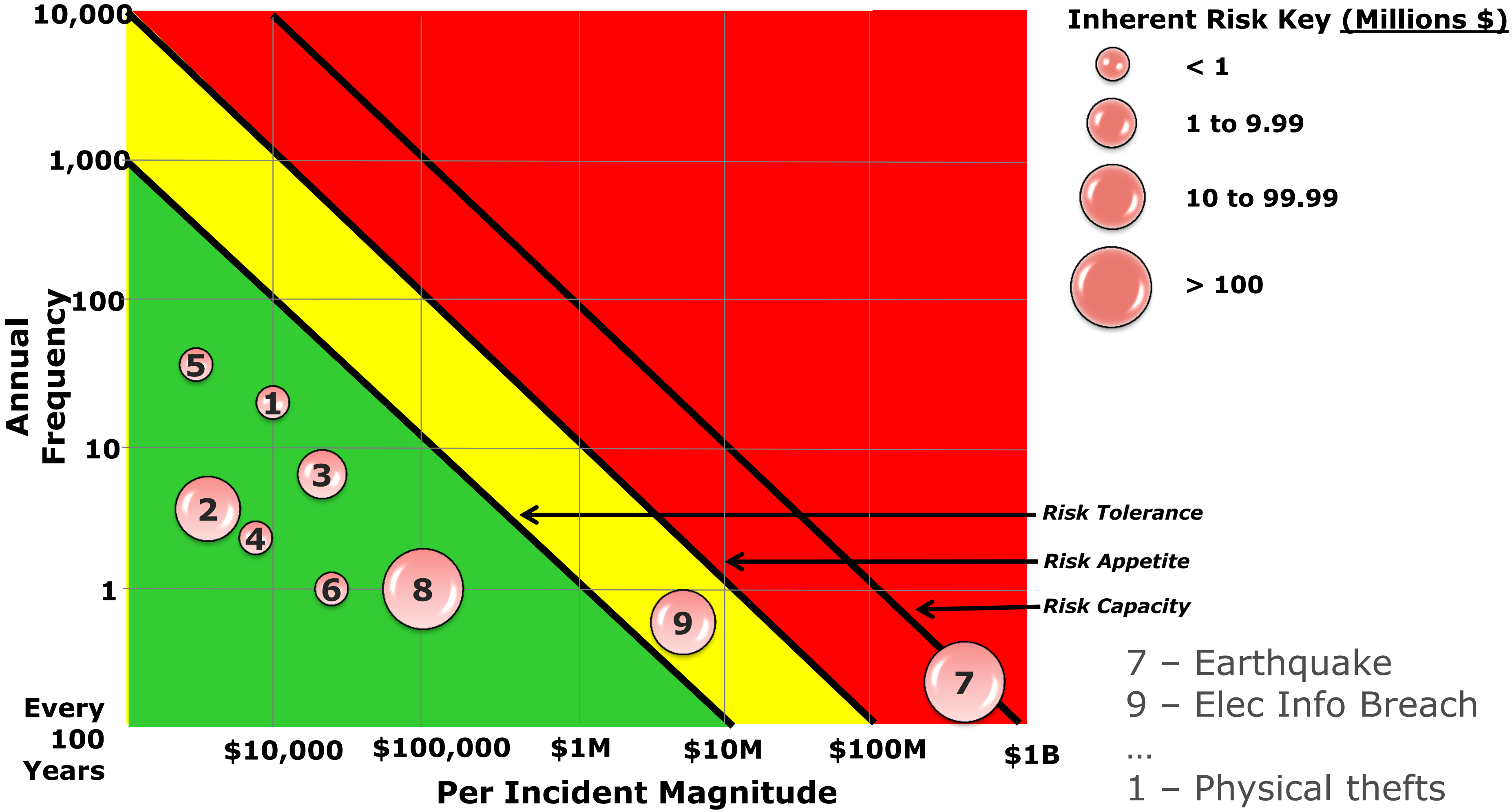
Risk Factor	Inherent Risk	Residual Risk
Production line interruption due to power failure	⬆	⬇
Information security breach	⬆	⬆

Risk-Metric Trend Line (# power outages)



© Copyright 2014 EMC Corporation. All rights reserved.

Residual Risk Distribution Against Boundaries & Inherent Risk Magnitude



7 – Earthquake

9 – Elec Info Breach

…

1 – Physical thefts

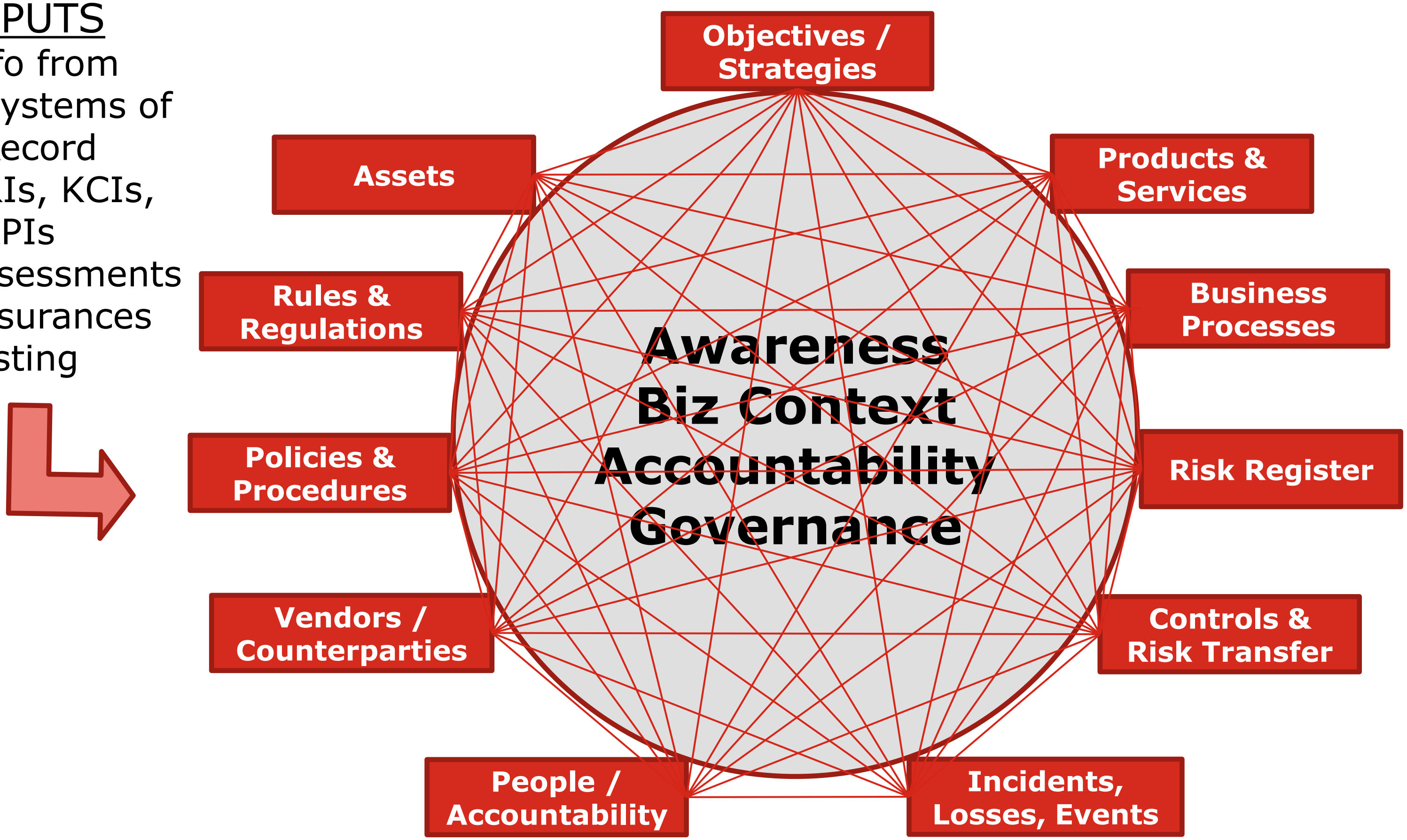
© Copyright 2014 EMC Corporation. All rights reserved.

What it takes to implement ERM?

© Copyright 2014 EMC Corporation. All rights reserved.

ERM Information Architecture

<u>INPUTS</u>
Info from Systems of Record
KRIs, KCIs, KPIs
Assessments
Assurances
Testing



<u>OUTPUTS</u>
Ownership
Exceptions, Incidents, Losses
Remediation Plans
Changes
Decision Workflow
Dashboards
Notifications
Reports

Operationalizes risk management practices across risk categories; Enables consistent risk decisions; Enables efficiencies across the 3 lines of defense; Fewer surprises; Institutionalizes knowledge; Better decisions; Promotes risk management culture; Provides positive assurance to stakeholders

© Copyright 2014 EMC Corporation. All rights reserved.

Foundational Issues

- Authority
- Program Scope & Purpose
- Terminology
  - What is Risk – both good and bad?
  - What is Control?
  - Risk Categories?
  - What does risk assessment mean?
- Roles and Functions
  - Ownership / accountability of risks, controls, risk-related policies
  - 3 Lines of Defense
  - Define Key Risk Management Roles
  - Risk Governance Committees
  - ENGAGE Stakeholders

© Copyright 2014 EMC Corporation. All rights reserved.

Foundational Issues (continued)

- Scope of framework elements
- Approach(es) to risk assessment
  - Risk category classifications
  - Inherent / Residual
  - Likelihood / Impact; Frequency vs. Likelihood
  - Volatility, Threats, Sources
  - Qualitative, Quantitative, Both
  - Business context boundaries
  - Top-Down / Bottom-Up Assessments / Unification
  - Existing and Emerging Risk – Workshops, Self-Assessments, Periodic assurance and testing

© Copyright 2014 EMC Corporation. All rights reserved.

Foundational Issues (continued)

- Rating Scales (Harmonized)
  - Risk Assessment
  - Internal, External, Regulatory Audit Issues
  - Incidents, Events, Losses, Near Misses
  - Visual representation
- Risk Appetite, Tolerance, & Delegated Authorities
  - Decision workflow
  - Exception handling & Escalation
  - Reporting

© Copyright 2014 EMC Corporation. All rights reserved.

Foundational Issues (continued)

- Communication Structure
  - Management Roll-up
  - Business Hierarchy Roll-Up
  - Financial Roll-up
  - Risk Governance Committee domain
- Information Management
  - Documentation of Efforts
  - ERM Framework Registers
  - Change control
  - Automation tools
- Formal Enterprise Risk Management Practices and Procedures

© Copyright 2014 EMC Corporation. All rights reserved.

A/D of Closer BCP-ERM Alignment

© Copyright 2014 EMC Corporation. All rights reserved.

Advantages from Integration with ERM

- Leverage common use of business processes & Information
- Greater visibility / advocacy for BCP
- Transparency of changes in infrastructure
- Consistent risk transfer purchases
- Expanded career path / ability to influence enterprise approach to risk management
- Criticality of Business processes informs third party criticality
- Can use BIAs to capture non-resiliency-related risk. Efficiency of streamlined information capture.

© Copyright 2014 EMC Corporation. All rights reserved.

Potential Disadvantages to BCP from ERM Integration

- Adherence to ERM policies and practices
- Taxonomy
- Rating Scales
- Assessment Approaches
- Audit Findings
- Remediation Plans
- Decision thresholds and decision trees
- Executive and Board Reporting
- More chefs in the kitchen

© Copyright 2014 EMC Corporation. All rights reserved.

Enhancing BIA, Additional Value to ERM

© Copyright 2014 EMC Corporation. All rights reserved.

Leveraging the BIA process for ERM

Strategic

1. What level of impact does this process have on the company's ability to achieve its strategic objectives?
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)
2. Does this process support key initiatives, customers or other significant and strategic activities?
   - App: Corporate Objectives, Info: KPIs

Financial

1. How significant does this process contribute to the generation of revenue or cost control?
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)
2. Is this process consistently in scope for Sarbanes Oxley testing?
3. Are there critical financial accounting transactions or reporting performed?
   - App: Business Process, Info: GL Account name, account balance.

Compliance

1. How significant are the external compliance obligations or contractual obligations that this process supports?
2. If this process was interrupted when would this impact occur? (N/A, 4 hours, 8 hours, etc.)

© Copyright 2014 EMC Corporation. All rights reserved.

Leveraging the BIA process for ERM

Data Confidentiality

1. How significant is the non-public personal information or internal confidential information supported by this process? (None, Low, Medium, High)
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)

Financial Reporting

1. To what degree could errors, if introduced through this process, affect the accuracy of the organization's financial statements, or subsidiary records?
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)

Fraud

1. To what degree could unauthorized manipulation of data managed by this process result in financial loss to the organization or its customers?
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)

Operational

1. Is this process highly technical, complex or highly transactional, or a critical part of larger supply chain?
2. Are significant assets, people, money or other resources needed to support this process?
3. Does this process have a material impact on the company's operations?
4. Would key employee turnover have a material adverse effect upon company operations?

© Copyright 2014 EMC Corporation. All rights reserved.

Leveraging the BIA process for ERM

Reputation

1. Does this process have a direct impact upon or interaction with external customers?
2. Does this process involve highly sensitive regulatory or compliance requirements that could impact reputation?
3. Is this process highly visible to media, press, analysts, shareholders?
   - Free Form Text Field: Describe any known impacts of unauthorized modification of data.

Third Parties

1. Does this process rely on critical third parties?
   - At what point would this process fail if the third party failed? N/A, 4 hours, 8 hours, etc.)

Life and Safety

1. How significant is this process for protecting health and welfare of employees, customers, and third parties?
   - If this process was interrupted, when would this impact occur? (N/A, 4 hours, 8 hours, etc.)

© Copyright 2014 EMC Corporation. All rights reserved.

Conclusion

© Copyright 2014 EMC Corporation. All rights reserved.

Summary

- ERM focuses on increasing likelihood organization will achieve objectives
- Business Continuity is a critical enterprise risk to achieving objectives
- Integration:
  - Creates unified message
  - Delivers advantages to ERM and BCP

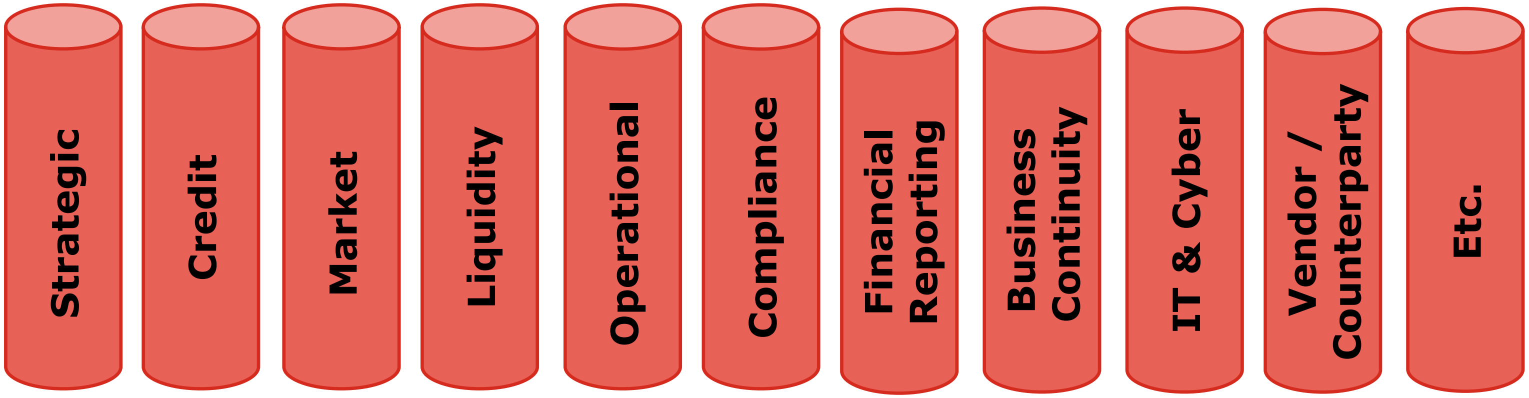
© Copyright 2014 EMC Corporation. All rights reserved.

RSA®

EMC^2®

Risk Management Inconsistency Arises

- Oversight Fragmented by Risk Type

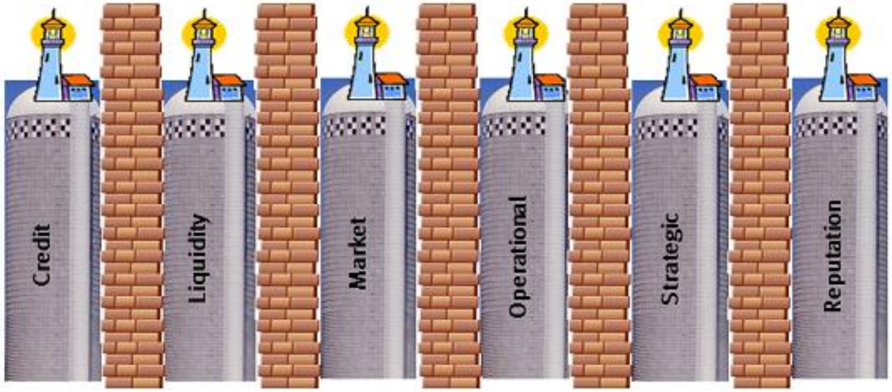


- Managed independently by LOB or Product / Service
- Variation in geographic approaches
- Managed with different and disconnected tools
- Business context & interconnectedness not always understood
- Volume and complexity of information outstrips resources

© Copyright 2014 EMC Corporation. All rights reserved.

Incomplete Knowledge of Risks

- No holistic repository of enterprise risks
- Emerging risks from external events
- Acquired risks from mergers & acquisitions
- New ventures (products, services, markets)
- Changing business process, technologies, & organizational structure
- Changes in institutional knowledge



© Copyright 2014 EMC Corporation. All rights reserved.

Inconsistent Risk Assessment

- Unclear or undefined risk taxonomy
- Some areas not performing risk assessments
- Different risk assessment approaches
- Different risk assessment scales
- Risk assessments that don't provide meaningful information

© Copyright 2014 EMC Corporation. All rights reserved.

Inconsistent Risk Decision Processes

- Risks without defined, well communicated, or enforced risk appetites and tolerances
- Varying risk tolerances across comparable risks
- Misalignment between different areas of enterprise
- Decisions based on bad information
- Decision processes not adequately formalized
- Changing risk not subject to timely decisions

© Copyright 2014 EMC Corporation. All rights reserved.

Suboptimal Risk Treatment

- Uncertain knowledge regarding correct balance of risk treatment vs. risk capacity, appetite, and tolerance
- Risks over-controlled
  - Excessive resource cost
  - Lost opportunities
  - Slow to respond
- Risks under-controlled
  - Surprises
  - Excessive losses

© Copyright 2014 EMC Corporation. All rights reserved.

Fragmented & Ineffective Risk Monitoring

- Non-existent monitoring of some activities
- Uncertainty about the key drivers of specific risks and the significance of the drivers
- Poor design (subjective, doesn’t capture scenarios)
- Frequency not consistent with risk volatility
- Process prone to error (manual/reliant on SMEs)
- Unaware of changing risk profile
- Inability to predict and avert surprises

© Copyright 2014 EMC Corporation. All rights reserved.

Poor Accountability & Risk Culture

- Risk concepts, terms, applicability, & importance not understood by managers
- Risk responsibilities not clearly communicated
- No visible link between manager’s risk responsibility and overall risk to organization
- Exceptions & issue escalation without consistent management feedback loop
- Risk taking & compensation not formally linked

© Copyright 2014 EMC Corporation. All rights reserved.

Demonstrating Effectiveness & Efficiency

- Satisfying Exec. Mgmt., Board, Auditors & Regulators
- All significant risks captured, assessed correctly, decisioned, treated, & monitored enterprise-wide
- Timely awareness & response to emerging/changing risk
- Understanding where weaknesses in ERM program reside & having active plans to remediate & mature
- No significant surprises

© Copyright 2014 EMC Corporation. All rights reserved.

Management Overhead, Cost, Inefficiency

- Spreadsheet risk management inefficient / prone to error
- Managers bombarded with multiple questionnaires and subject to multiple audit and compliance tests
- Analysts spend too much time on admin tasks
- Knowledge not captured / leveraged for multiple purposes
- Reporting burdensome

© Copyright 2014 EMC Corporation. All rights reserved.