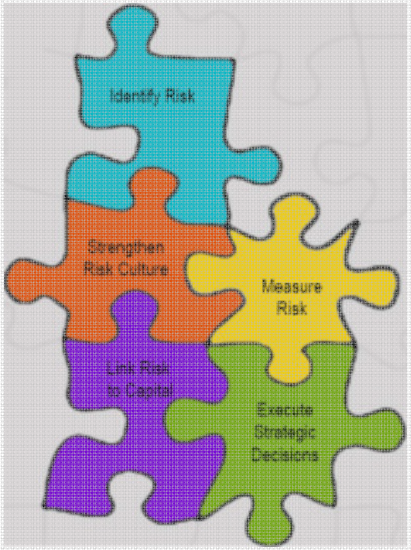
Practices in Enterprise Risk Management

John Foulley
Risk Management Practices Head
SAS Institute Asia Pacific

What is ERM ?

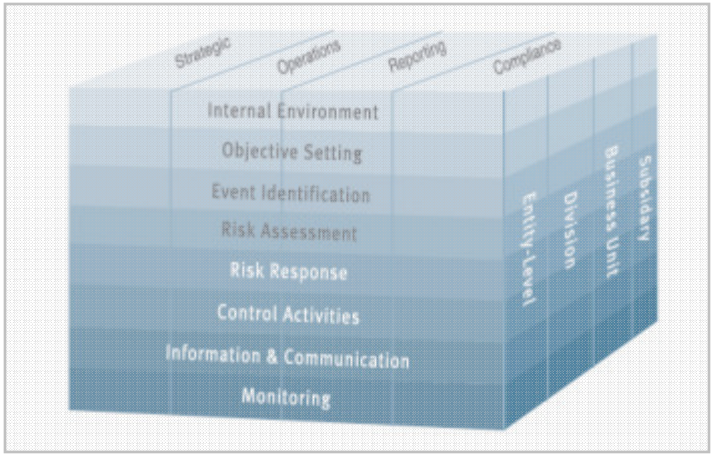
Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable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



- Is a *process* – it's a means to an end, not an end in itself
- Is *effected by people* –involves people at every level of an organization
- *Is applied across the enterprise, at every level and unit*
- *Is designed to identify events potentially affecting the entity and manage risk within its risk appetite*
- *Provides reasonable assurance to an entity's management and board*

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

ERM – COSO Framework



1. ERM framework is in form of three dimensional matrix in shape of a cube. The matrix includes four categories of objectives at the top strategic, operations, compliance & reporting

2. There are eight components of ERM are represented by horizontal rows. Each component row “cuts across" and applies to all four objectives categories.

3. The entity , its divisions and business units are depicted as third dimension. ERM is equally relevant to an entire enterprise or to an individual business unit.

4. No two entities will, or should, apply enterprise risk management in the same way. ERM capabilities and needs differ dramatically by industry and size, and by culture and management philosophy

5. However, all entities need each of the components to maintain control over their activities, one company's application of the ERM framework – often will look very different from another's.

6. ERM is not an end in itself, but rather an important means to achieving its objectives. It does not operate in isolation in an entity, but rather is an enabler of the management process.

Management Activities	Management Activities	Enterprise Risk Management
Establish mission, values and strategy	✓	
Apply enterprise risk management in setting strategy	✓	✓
Establish objective-setting processes	✓	✓
Select entity-level and activity-level objectives	✓	
Set performance measures	✓	
Establish internal environment	✓	✓
Establish risk appetite and set risk tolerances	✓	✓
Identify potential events	✓	✓
Assess risk impact and likelihood	✓	✓
Identify and assess risk responses	✓	✓
Select and execute risk response	✓	
Effect control activities	✓	✓
Inform and communicate with internal and external parties	✓	✓
Monitor the presence and functioning of the other components of enterprise risk management	✓	✓

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Internal Environment - COSO

The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment comprises many elements, including

Risk Management Philosophy is reflected in its policy statements and other communications. Importantly, management reinforces the philosophy not only with words but with everyday actions as well.	• Mission, Values, Strategy • Risk Governance Policy
Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity's risk appetite.	• Risk based Planning • Risk Tolerance
Risk culture is the set of shared attitudes, values and practices that characterize how an entity considers risk in its day-to-day activities. Risk culture flows from the entity's risk philosophy and risk appetite.	• Corporate Governance Code • Management Action
Organizational structure provides the framework to plan, execute, control and monitor its activities. It includes defining key areas of authority and responsibility and establishing appropriate lines of reporting.	• Centralized / Decentralized • Product/ Geography / Industry
Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, as well as limits to their authority.	• Reporting relationships • Authorization protocols
Human resource practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating and taking remedial actions send messages to employees.	• Recruitment & Training Policy • Code of Conduct

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Internal Environment – Solution

Entity Definition & Structure

- Document Organisational Hierarchy
- Business Component- Reporting
- Associate Business Components

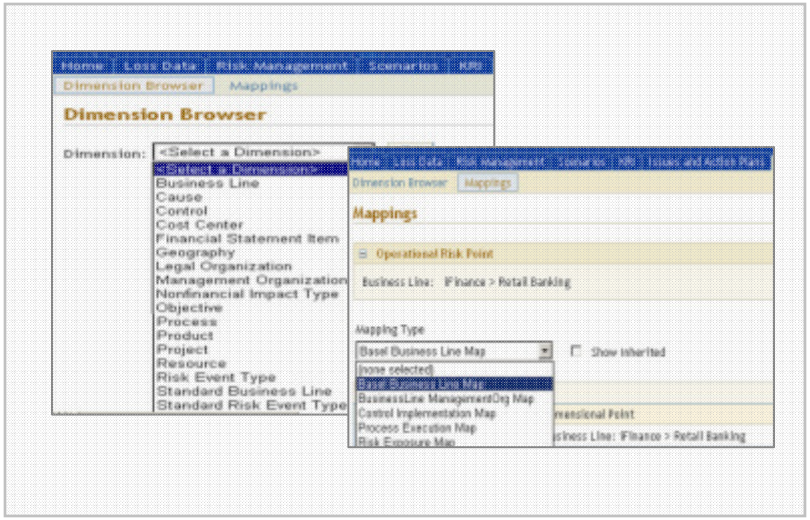
A great challenge of risk management is to **situate risk-related data** correctly within an organization. Simplistic models of business structure can lead to serious problems in managing risk. Monitor models the **multidimensional complexity** of a real organization in terms of these **three organizational spaces**:

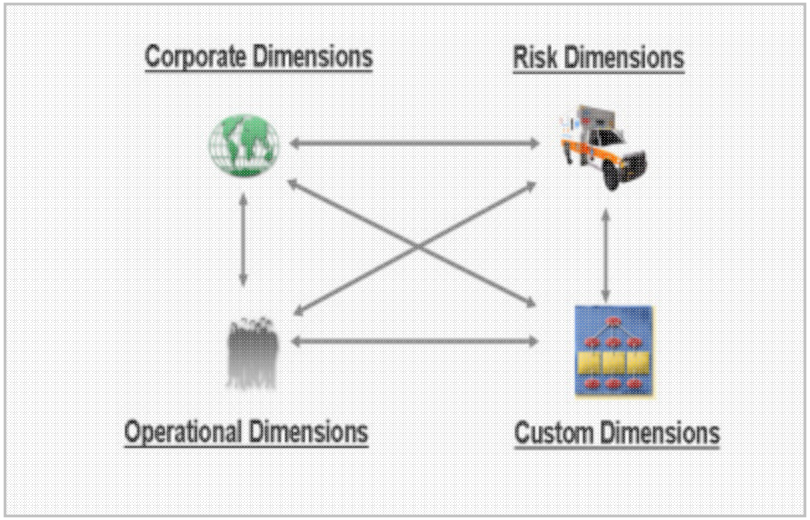
Structural space, which includes reporting structure, legal structure, business lines, cost centers, and geographies

Operational space, which includes business processes, resources, and products

Risk-analysis space, which includes categories of risks or events, causes, and control frameworks

Monitor models the web of relationships among these spaces. Within this rich model of business and risk structure, and replicates the internal environment of the organisation.





Internal Environment – Solution

Entity Definition & Structure

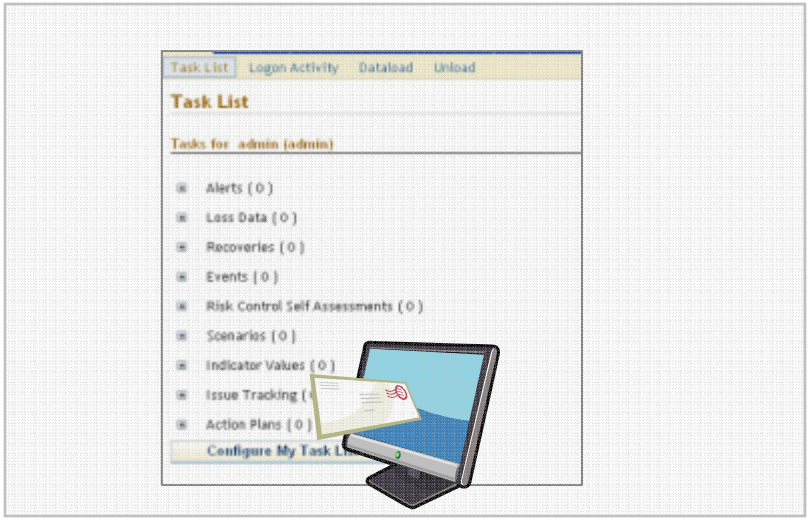
- **Integrated GRC**
- **Risk Culture**

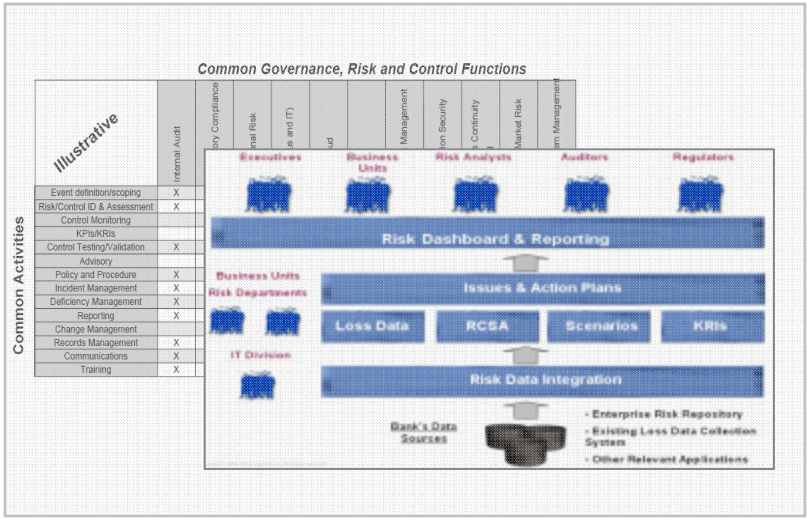
Integrate GRC activities and leverage common people, processes, technology, and information enterprise-wide,

- **Event Identification • Risk Assessment • Control Testing/ Monitoring • KRI / KPI**
- **Loss Incident • Risk Treatment- Issues & Action Plans • Dashboard**

Establishment of risk culture requires that the tools for collecting and managing risk data be available in the hands of each employees in every department. The Web-based user interface can be used by anyone with access to a Web browser

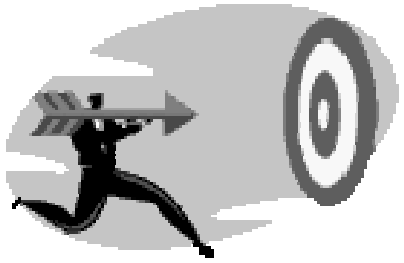
- **Email Notification**
- **Simple Task List**
- **Scalable to large no. of users**





Objective Setting- COSO

Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity's activities.



Strategic objectives are high-level goals, aligned with and supporting the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders.

Related Operations Objectives pertains to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss.

Related Reporting Objectives pertains to reliable reporting which, provides management with accurate and complete information appropriate for its intended purpose and supports management's decision making and monitoring

Related Compliance Objectives establish minimum standards of behavior pertains based on applicable laws and regulations, which the entity integrates into its daily activities and operations.

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives.

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Objective Setting – Solution

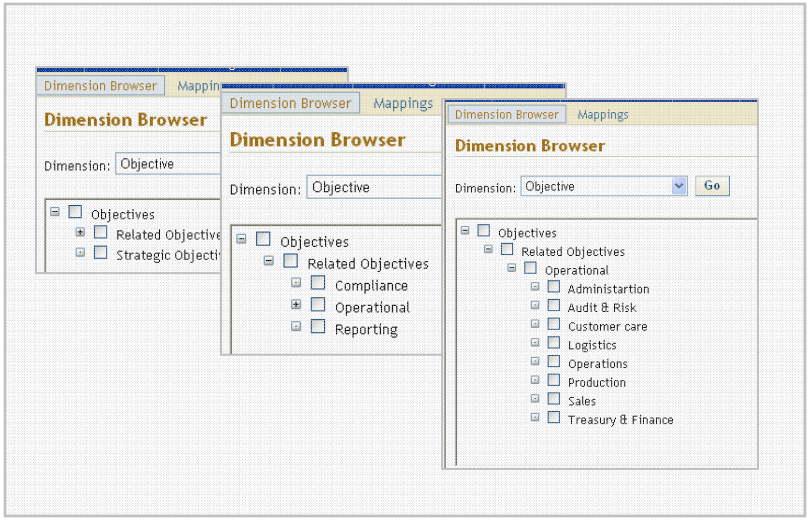
Entity Objectives

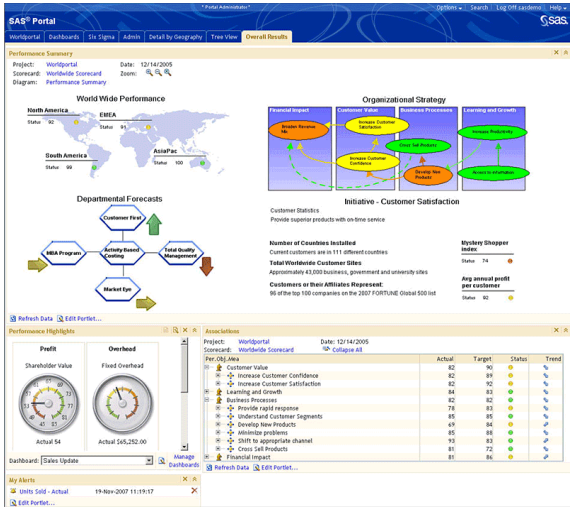
- Document Objectives
- Reliable Reporting
- Legal compliance

• Map Objectives to Entity / Controls / Process • KRI / KPI monitoring

• Automatic consistency check • Data Validation • Structural relationships and referential data used to streamline data-entry process

• Business structures / Process / Risk mapping • Associate controls with financial assertions • Audit Trails





Strategic Objective Setting – Solution

Entity Objectives

- Document Objectives
- Reliable Reporting
- Legal compliance

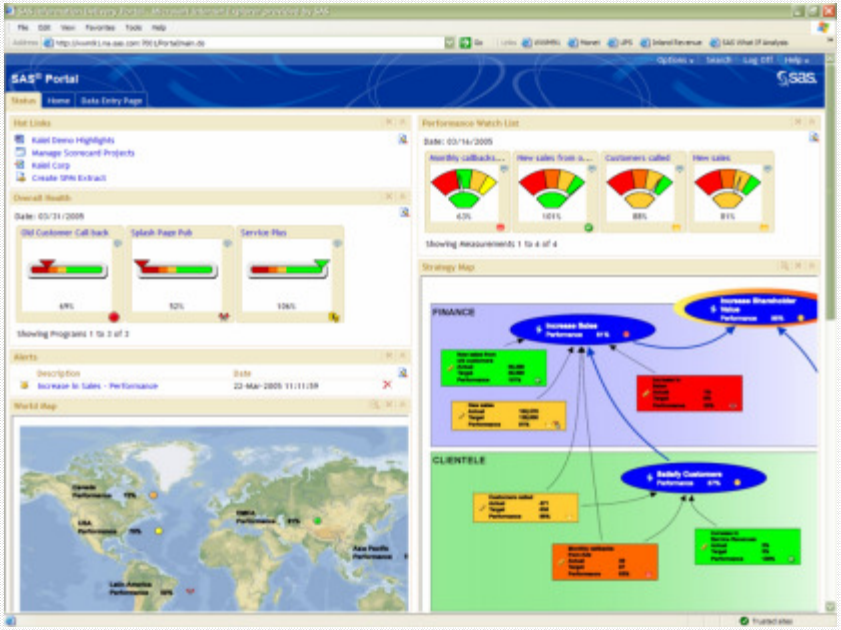
Certified by the **Balanced Scorecard** Collaborative as meeting the functional requirements for use as a Balanced Scorecard management system

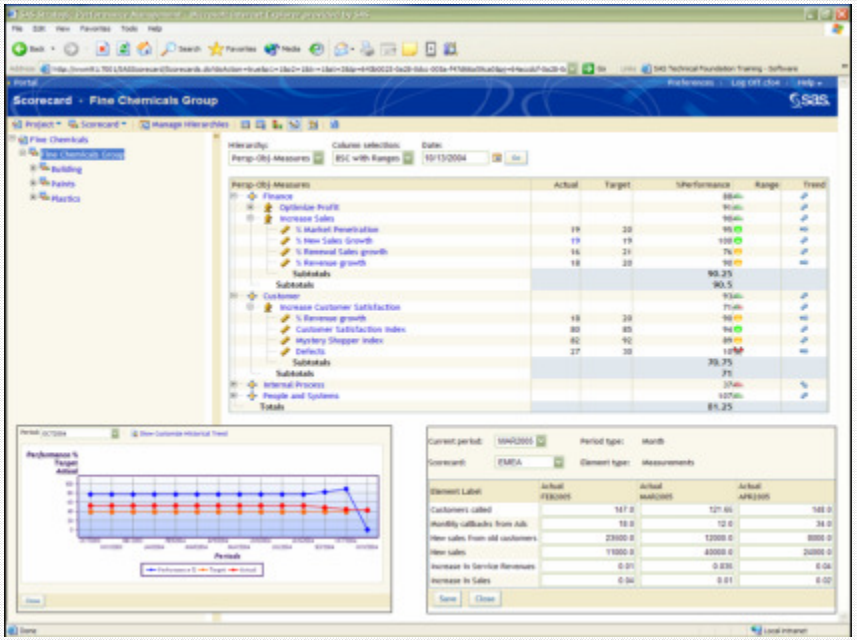
Fully **web-based**, drill-down & collaboration capability~ thresholds & alerts, document & comments management.

Simple **web data entry** to enable a large group of users to capture KPI results

Cater to **complex scoring**, **aggregation** and/or weightage computation

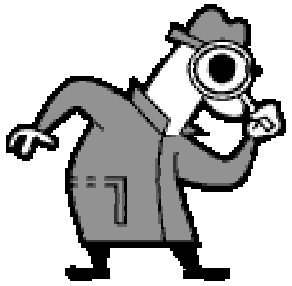
Can be easily tailored **for other management frameworks (e.g. Enterprise Risk Management, 6-sigma, Malcolm Baldridge, SQA, EVA)**





Event Identification - COSO

A myriad of external and internal factors influences how events could potentially affect strategy implementation and achievement of objectives. As part of enterprise risk management, personnel recognize the importance of understanding external and internal factors and the type of events that can emanate there from.



Event inventories are detailed listings of potential events common to companies within a particular industry, or to a particular process or activity common across industries.

Escalation or threshold triggers alert management to potential areas of concern by comparing current transactions, or events, to predefined criteria. Once triggered, an event may require further assessment or an immediate response.

Leading event indicators – By monitoring data correlated to events, entities identify the existence of conditions that could give rise to an event – often referred to as leading event indicators.

Loss event data methodologies – Repositories of data on past loss events are a useful source of information for identifying trends and root causes. Once a root cause has been identified, management can provide effective solution

Process flow analysis – By considering the internal and external factors that affect inputs, or activities within a process, an entity identifies events that could affect achievement of process objectives.

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Event Identification – Solution

Event Identification

- Event Repository / Risk factors
- Leading Indicators / Scenarios
- Incident Management

Event Repository Risk / Opportunities .Identify risk at entity / process dimension

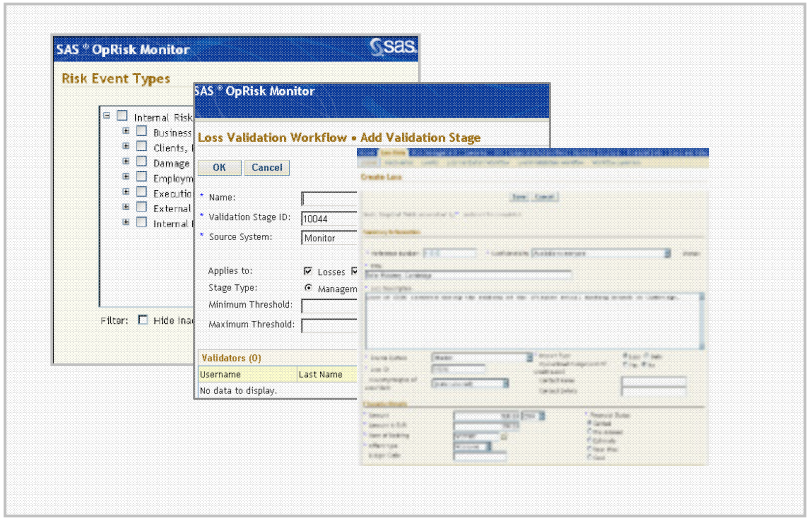
• **Internal risk events**• **Map to Industry standard risk events**

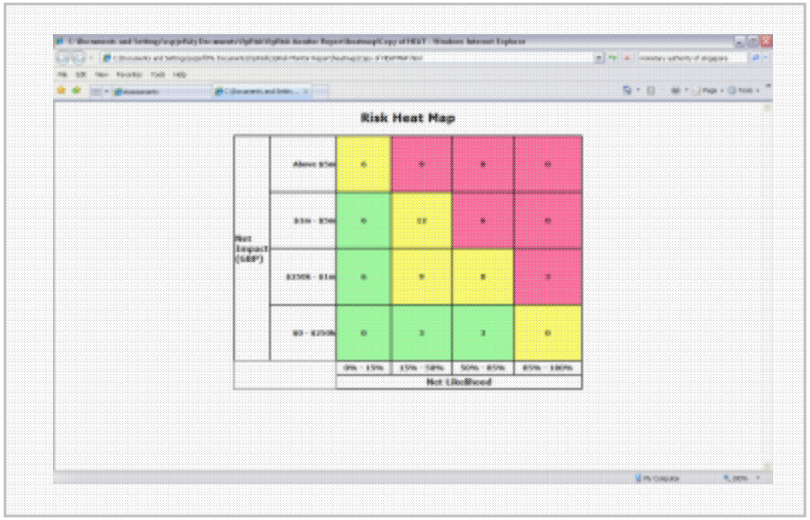
KRI/ KPI process enables one to capture quantitative performance information

• **Create a KRI / KPI definition**• **Observation validation workflow**• **Request observation**• **Validate observation**

Incident database to capture loss event

• **Capture Event**• **Record loss effects / causes** • **Conditional Validation workflow**• **Record Recoveries**





Risk Assessment & Response - COSO

Risk assessment allows an entity to consider the extent to which potential events might have an impact on achievement of objectives. Management should assess events from two perspectives – likelihood and impact– and normally uses a combination of qualitative and quantitative methods

Inherent & residual risk-Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management responds to the risk.

Estimating Likelihood and Impact Uncertainty of potential events is evaluated from two perspectives – likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect.

Correlated Events - While the impact of a single event might be slight, a sequence of events might have more significant impact. Management may use scenario analysis to assess the effects of multiple events.

Risk Responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management considers costs and benefits, and responds to brings likelihood and impact within the desired risk tolerances.

Implementation Plan -Once management selects a response, it may need to develop an implementation plan to execute the response and recalibrate the risk on a residual basis.

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Risk Assessment - Solution

Risk Assessment

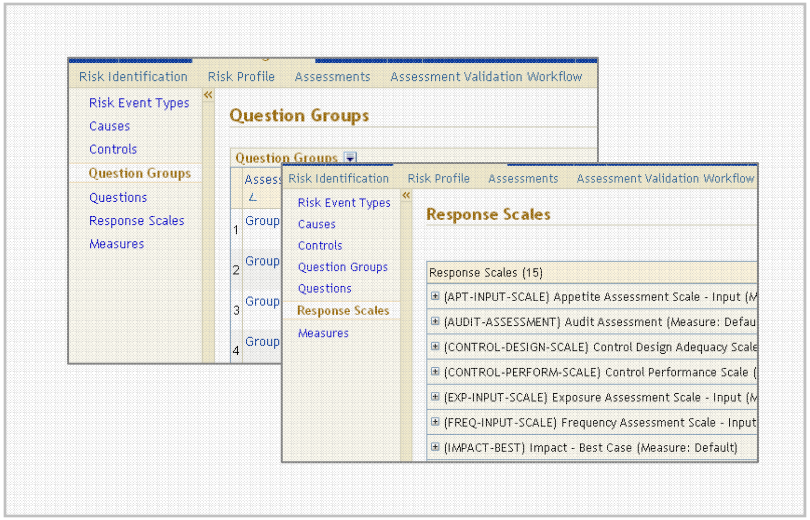
- Identify Risk & Risk Drivers
- Assessment schedule & items
- Automated Questionnaire / workflow

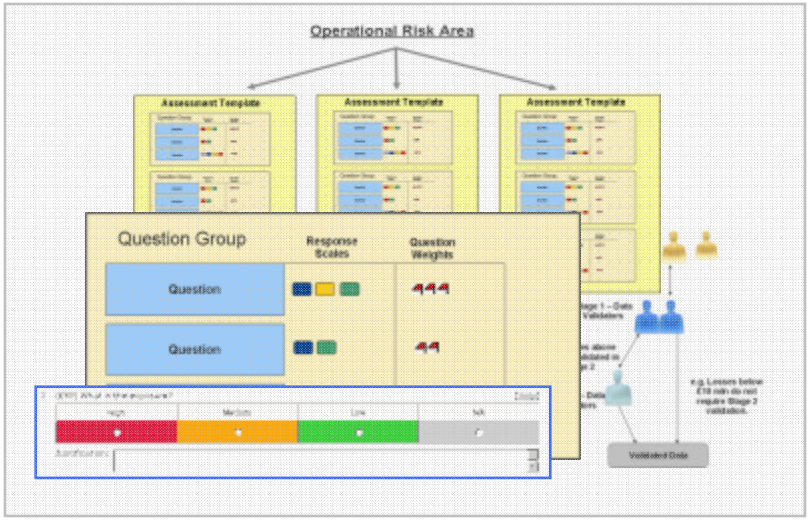
This process involves sending questionnaires to the appropriate people within an organization and collecting their responses.

•**Create and organize questions and question groups.** • **Map question groups to assessment items** • **Identify risks at operational risk points.**

• **Create questionnaire templates**• **Define the assessment validation workflow** • **Create and conduct the assessment**

Flexibility to define question , categories , assessment area, distribution mechanism and assessment area . Monitor assessment schedules, risk profiles and action plan in real time.





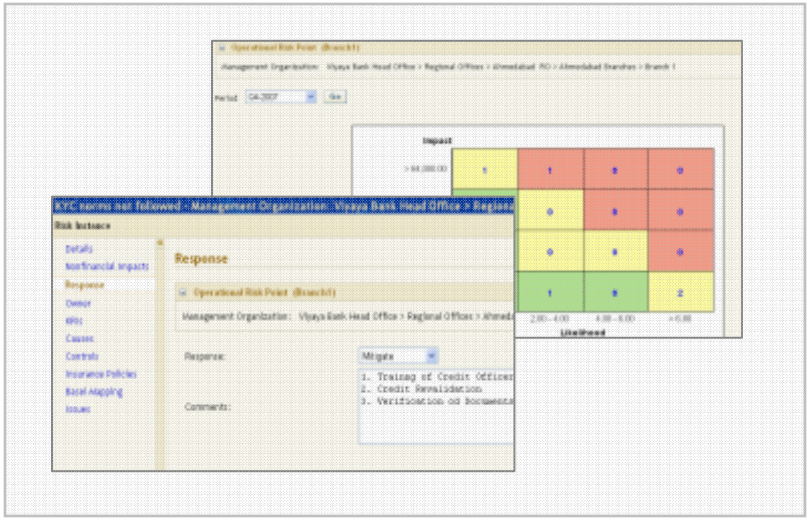
Risk Response - Solution

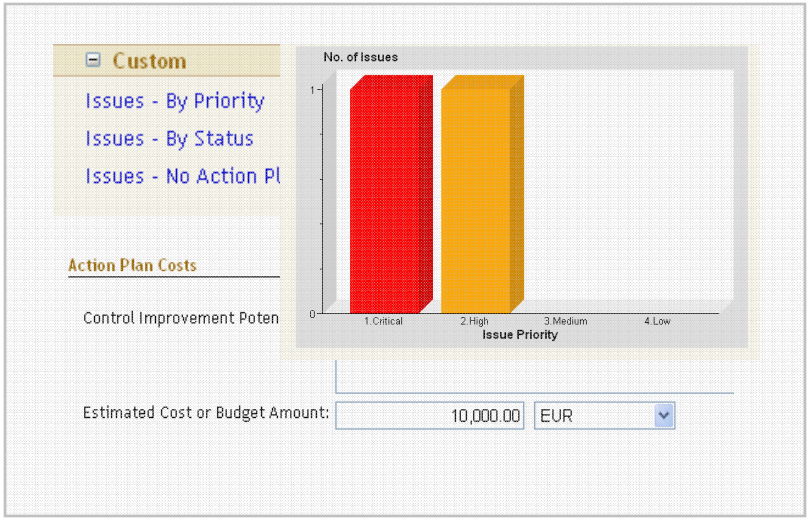
Risk Response

- **Risk Profile Heat Map**
- **Issues & Action Plan Tracking**

- Identifying Risk Response
- Action Plan Implementation
- Assessing the Costs Versus Benefits
- Portfolio View

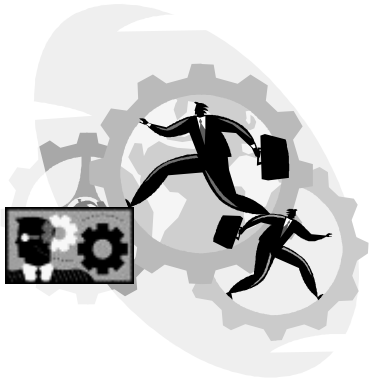
•Risk Profile • Inherent Risk Map • Residual Risk Map.• Escalation of issues. Corrective action plan • Monitoring of corrective action plan





Control Activities - COSO

Control activities are policies and procedures, which are the actions of people to implement the policies, to help ensure that management's risk responses are carried out. Control activities are applied with respect to each of the four categories of objectives – strategic, operations, reporting and compliance.



Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly. Control activities are part of the process by which an enterprise strives to achieve its objectives.

Control activities usually involve two elements: a **policy** establishing what should be done and **procedures** to effect the policy. A procedure will not be useful if performed mechanically and without a sharp, continuing focus.

General controls include controls over **information technology** management, information technology infrastructure, security management and software acquisition, development and maintenance. These controls apply to all systems

Application controls are designed to ensure completeness, accuracy, authorization and validity of data capture and processing. Individual applications rely on effective operation of controls over **information systems**.

The complexity of an **entity**, and the nature and **scope of its activities**, affect its control activities. Complex organizations with diverse activities may face more difficult control issues than simple organizations with less varied activities.

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

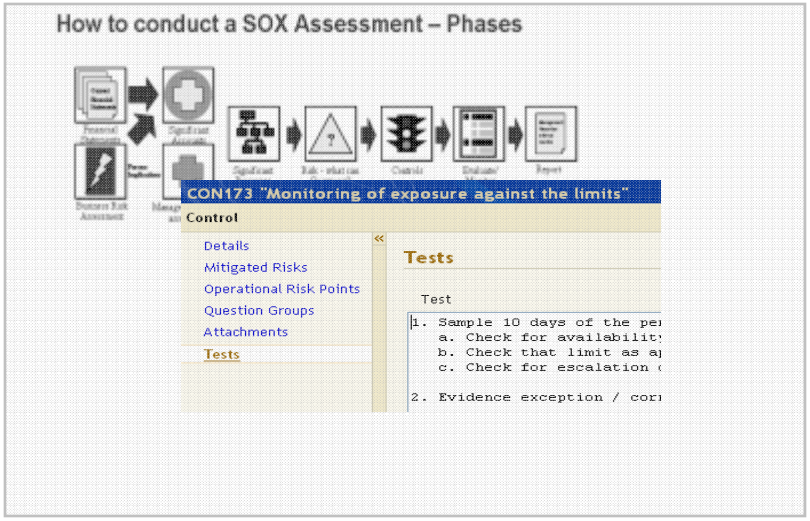
Control Activities - Solution

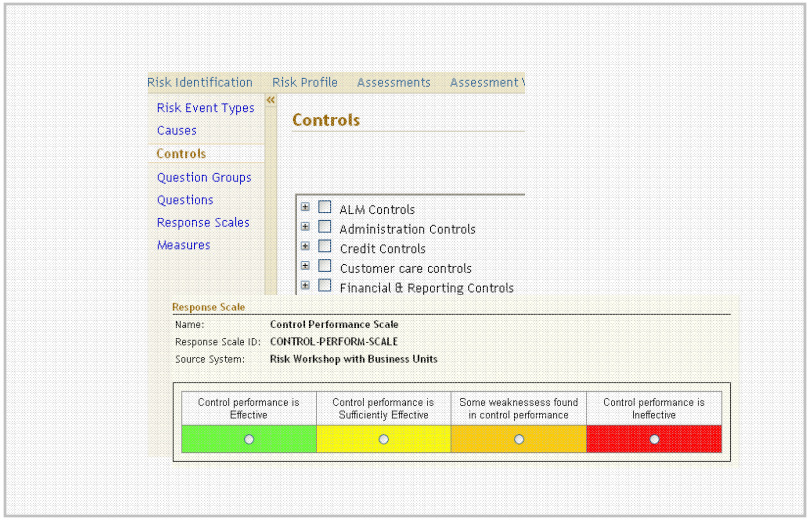
Identifying Controls

- Mapping controls to risk / process
- Design / Operating Effectiveness

- Identify controls
- Map Controls to Process / risks
- Map Process to Financial Statement Items
- Design Effectiveness of controls
- Operating Effectiveness of controls

•Control Profile • Residual Risk Map • Escalation of issues . Corrective action plan • Monitoring of corrective action plan •Control testing





Information- COSO

Pertinent information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information about external events providing information for managing enterprise risks and making informed decisions relative to objectives.

Information is needed at all levels of an organization to **identify, assess and respond** to risks, and to otherwise run the entity and **achieve its objectives**. An array of information is used, relevant to one or more objectives categories.

An organization's information **systems architecture** must be sufficiently flexible and agile to **effectively integrate** with new customers and business partners. Information systems often are **fully integrated** into most aspects of **operations**.

Web and web-based systems are common. These applications facilitate access to information previously trapped in functional or **departmental silos** and not practically available for **widespread management** use.

Increasing **dependence** information systems and data-driven automated decision systems and processes, **data reliability** is critical. **Inaccurate data** can result in unidentified risks or poor assessments and bad

Communication is inherent in information systems. Information systems must provide information to **appropriate personnel** so that they can carry out their **operating**, **financial reporting** and **compliance** responsibilities.

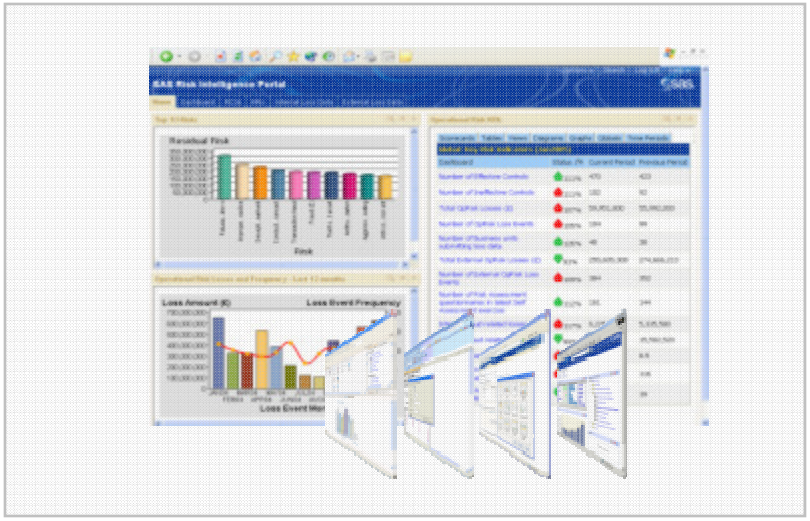
Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Information- Solution

Information

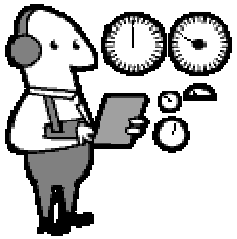
- Internal / Regulatory Reporting
- Dashboards
- System Integration

- Data Integration Server to integrate external data into ERM Database
- Data Confidentiality / Restricted Access
- BI Server empowers users to access information in the format they need
  - **Web Report Studio**
  - **OLAP Viewer**
  - **Dashboard**
  - **Office Addin**
  - **Delivery portal**
- Transformed data for reporting needs and optimal data mining performance
  - **Specified Pre-Built Reports**
  - **Design Custom Reports**
  - **Dashboards**
  - **Self Servicing reports**



Monitoring- COSO

Enterprise risk management is monitored – a process that assesses the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the normal course of management activities.



Ongoing monitoring is built into the normal, recurring operating activities of an entity. Ongoing monitoring is performed on a **real-time basis**, **reacts dynamically** to changing conditions and is ingrained in the entity.

Many activities serve to monitor the effectiveness of enterprise risk management These include regular management and **supervisory activities**, **variance analysis**, **stress testing**, **comparisons**, **reconciliations** and other routine actions.

While **ongoing monitoring procedures** usually provide important feedback on the effectiveness of other ERM components, it may be useful to take a **fresh look** from time to time, focusing directly on ERM effectiveness.

Providing needed information on enterprise risk management **deficiencies** to the **right party** is critical. **Protocols** should be established to identify what information is needed at a particular level for effective decision making.

Senior managers should be apprised of risk and **control deficiencies** affecting their units \ where assets with **monetary value** are at risk, where the or where important **financial reconciliations** are not performed correctly.

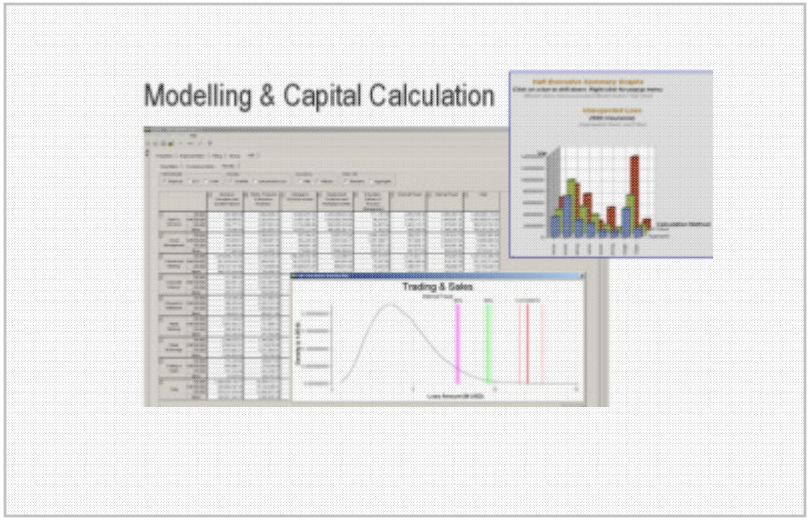
Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

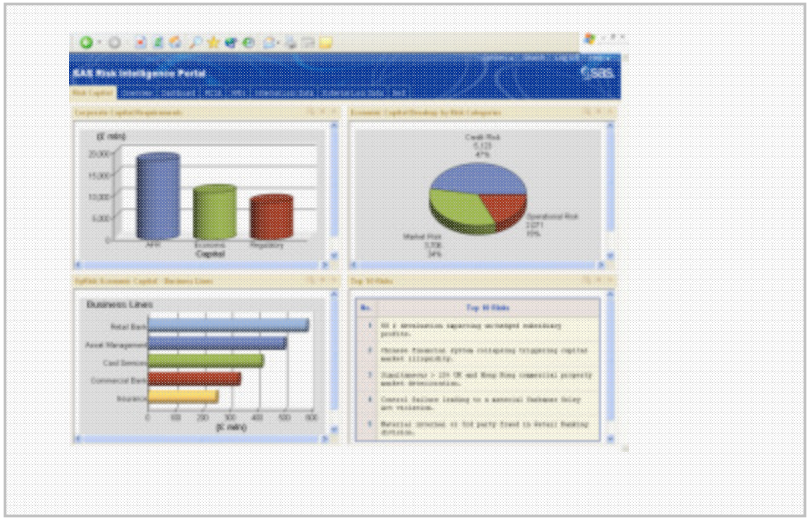
Monitoring- Solution

Monitoring

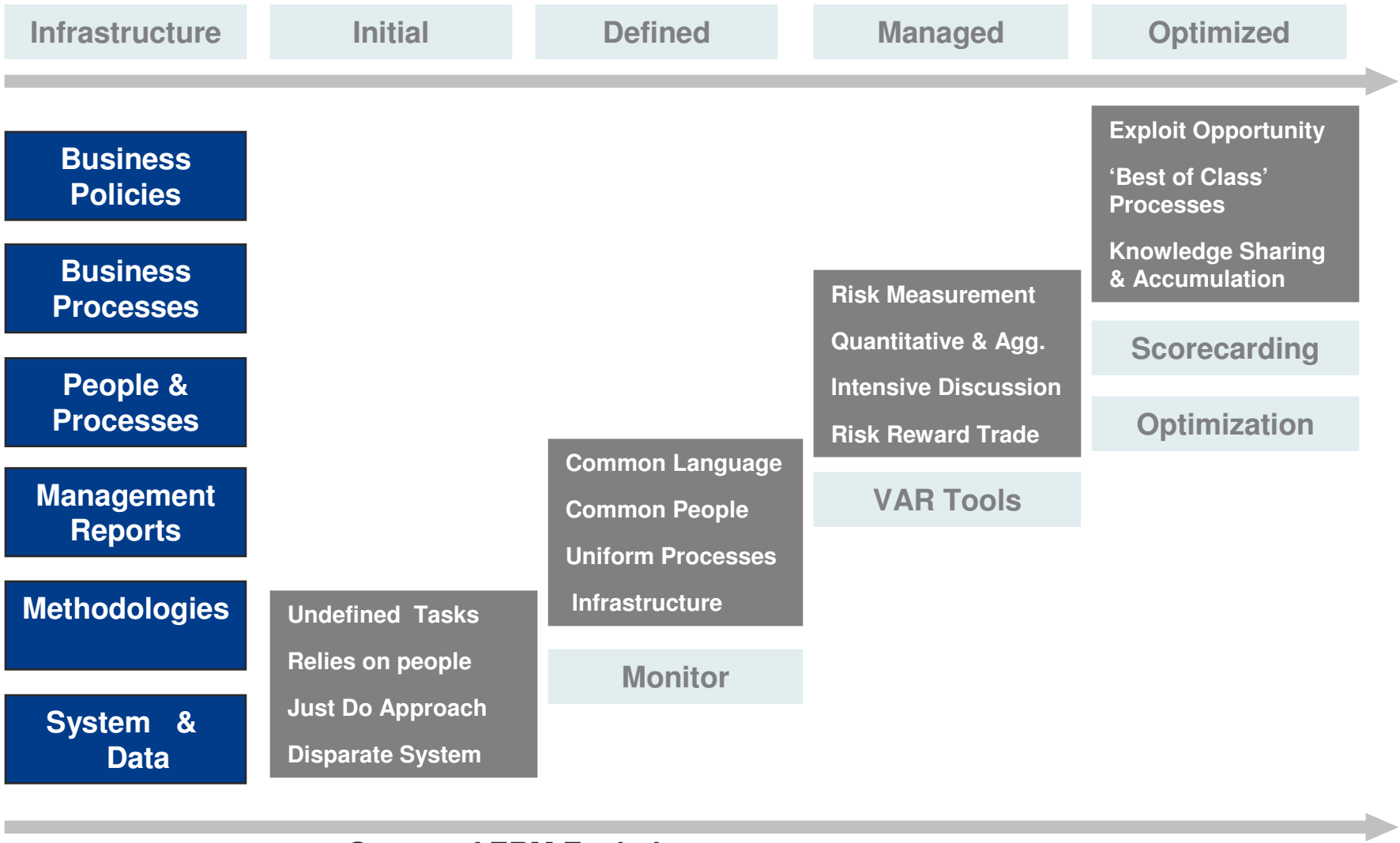
- VAR Exposure
- Reporting Protocols

- Building Exception reports / Monitoring KPI's
- Portals for ERM reporting to Compliance ,Business ,Audit
- Monitor VAR exposure for various business risks /RAROC
  - **Market Risks**
  - **Business Risks**
  - **Credit Risks**
- Define KPI/KRI • KPI/KRI Thresholds
- Reporting Protocols





ERM Process Evolution



Source: Adapted from the Capability Maturity Model: Guidelines for Improving the Software Process, Carnegie Mellon University Software Engineering Institute, 1994

End

THE POWER TO KNOW.®