iSPIRAL

RCMS PLATFORM

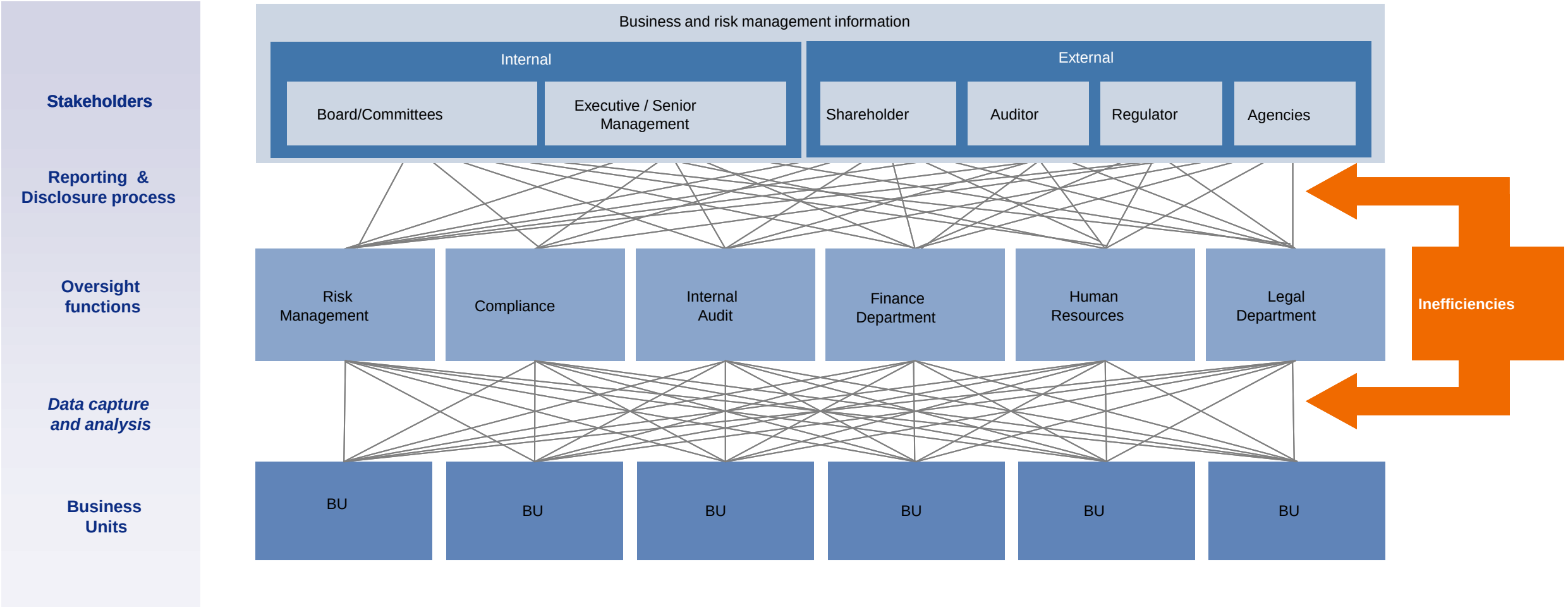
Envisioning the future of RegTech

01.

Introduction

Complexity of Risk and Compliance Management Processes

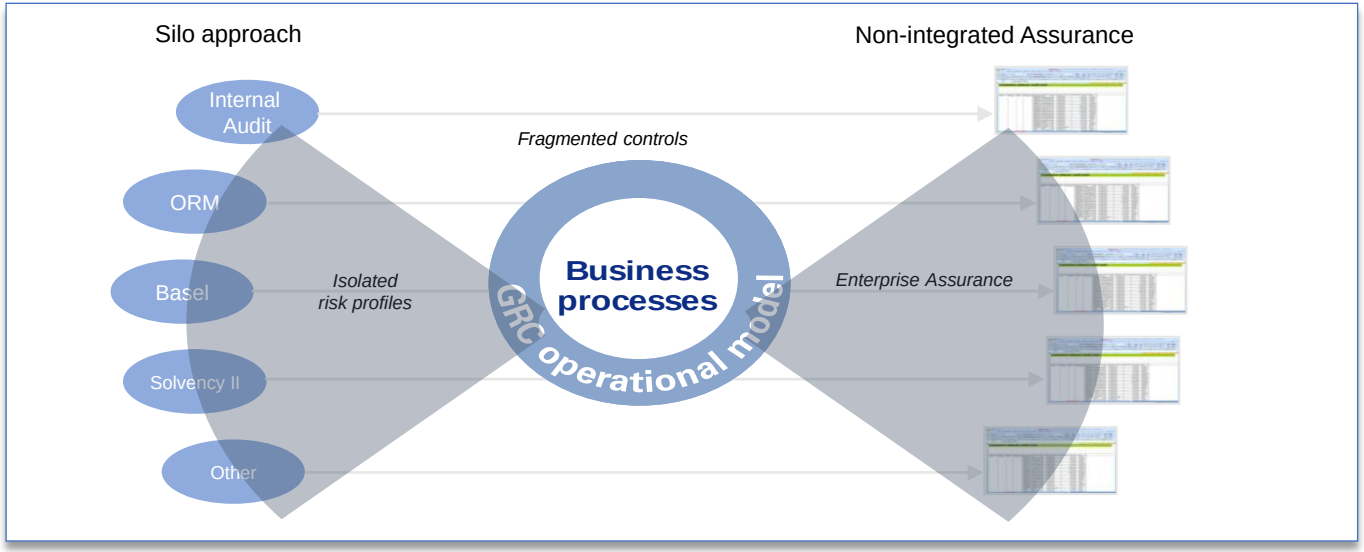
Increasing regulatory requirements have resulted in complex risk and compliance management processes



The Integrate approach , the key for success

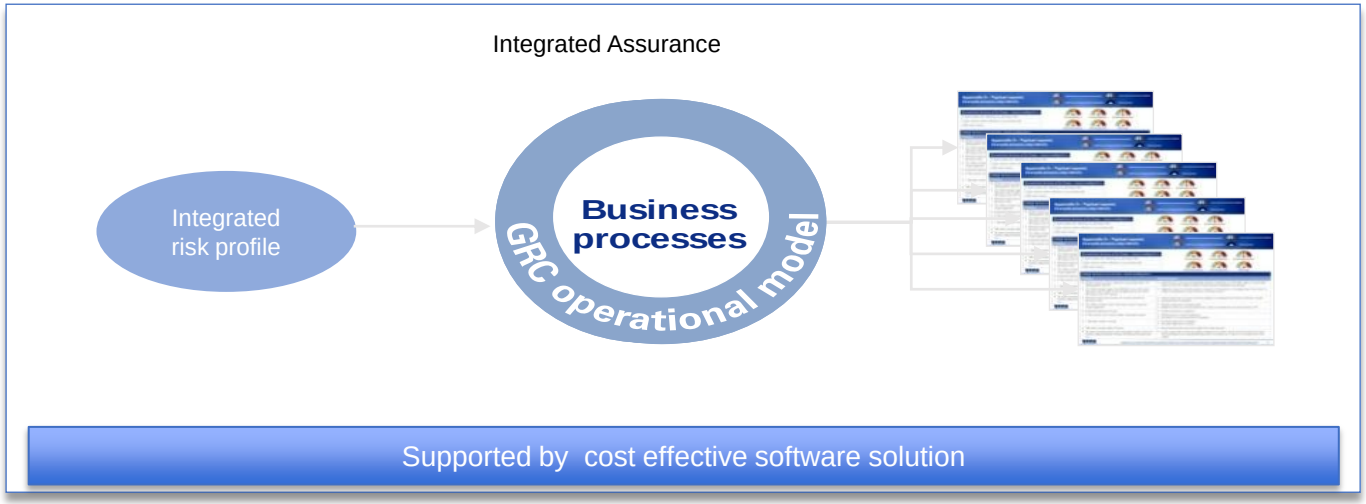
Non-Integrated Regulatory Compliance Assurance

- Different laws and regulations determine the risk profile in isolation
- Non-integrated control frameworks (silos)
- Fragmented controls for different purposes
- Controls mostly manual, detective and add-on
- Reviewed by a separate risk department, not by management
- Reporting mostly manual, supported by Excel
- Time consuming manual processes



Integrated Assurance

- Integrated risk profile
- Integration of the different control frameworks
- Controls documentation integrated in the system
- Efficiency monitored via 'dashboard reporting'
- Management is on top of the business processes
- Integrated compliance and risk management
- Embedded in business operations
- Comprehensive mitigation actions monitoring



02.

The solution

The Business case: Key Benefits of Risk and Compliance Process Automation

Intangible Benefits

- Improved Gap Detection and Mitigation
- Reduced Operating Risk
- Reduced Risk of Penalties, Fines Due to Noncompliance
- Improved risk transparency due to convergence
- Improved Reporting
- Improved management through automation

Tangible Benefits

- Reduced Risk Assessment Effort
- Reduced Compliance Effort
- Optimized Business Processes
- Automated Security and Controls Monitoring
- Promotes a risk culture increasing risk awareness
- Consolidation of risk and control frameworks

Governance, Risk and Compliance Model

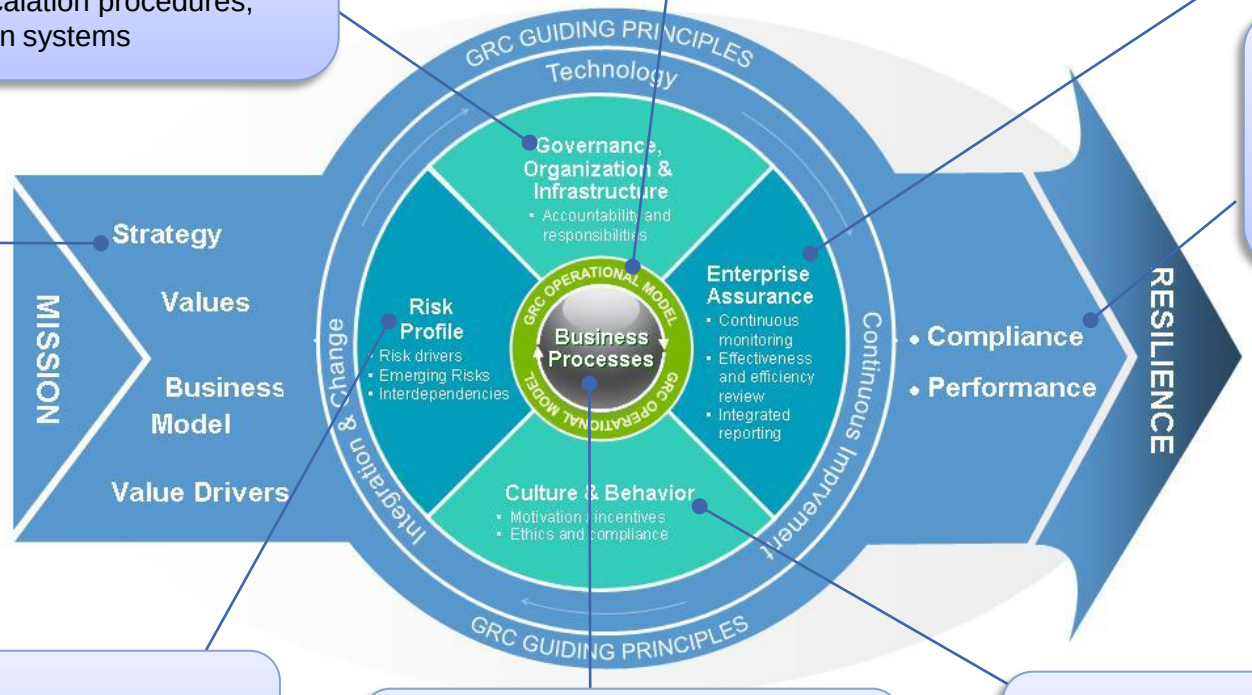
Governance, Organization & Infrastructure is the structuring and management of oversight structures, roles and responsibilities and resources, escalation procedures, and information systems

Operational Model covers the embedding of controls and reporting into the organization's business processes

Enterprise Assurance is the coordinated reporting and monitoring of the controls

Compliance & Performance provides internal and external monitoring of key risks and controls

Strategy is the development and planning of the business objectives. This is an input.



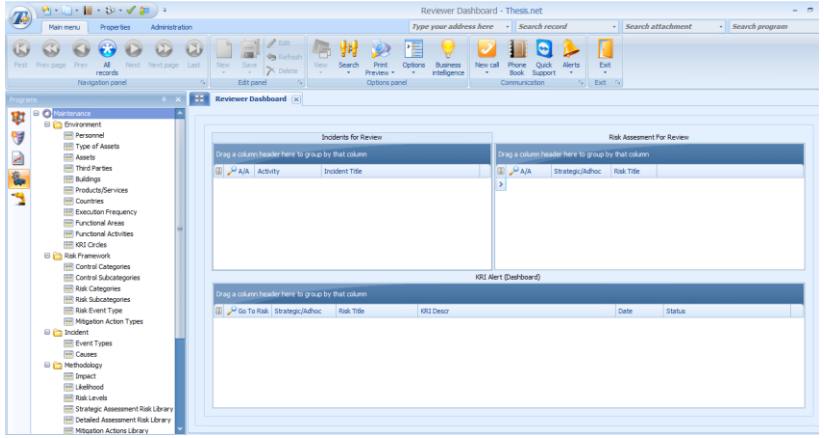
Risk Profile is the assessment of exposure areas and potential impacts

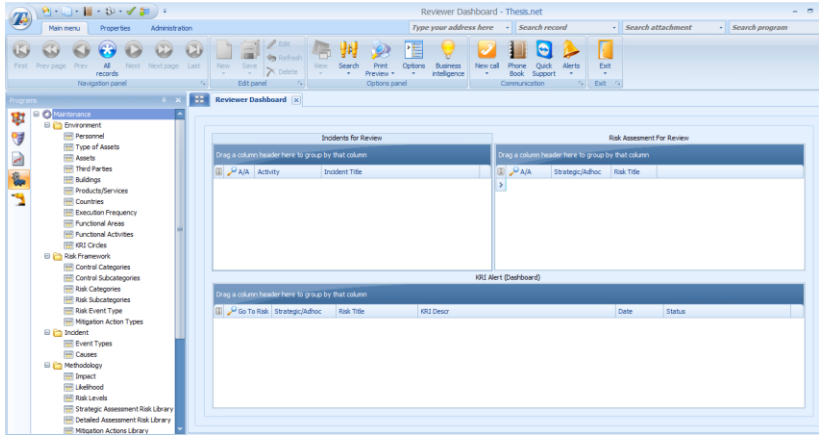
Business Processes are at the core of the holistic model where transactions and control activities are performed

Culture & Behavior is the embedding of the various aspects of governance risk and compliance into the organizational functions

The Risk and Compliance Management System (CMS)

- The Risk and Compliance Management System (RCMS) software solution is a specialized system that has been developed based on the experience drawn from our risk and compliance management professionals and the needs of our clients.
- The solution automates the core steps of a risk and compliance management process based on the Governance Risk and Compliance Model while implementing a simple and easy to use approach.
- It can be utilized to automate the Enterprise Risk Management, Information Security Risk Management (e.g. based on ISO 27001), Business Continuity Risk Management and any other similar risk management and compliance management processes.
- RCMS is a unified platform that can assist organizations meet their risk and compliance management objectives.





The RCMS Application : Key Functionality Concepts

Risk Management

- Strategic risk assessment
- Detailed / process risk assessment
- Risk surveying, rating and monitoring, Key Risk Indicators
- Multiple risk profile definition

Incident Management

- Incident reporting, registering and management
- Incident valuation and analysis
- Link to risk management
- Incident impact & actions definition

Compliance Management

- Control documentation and evaluation
- Actions / requirements / audit findings management
- Centralized actions monitoring

Workflow

- Task delegation
- Review and approval
- Custom alerts
- Roles and responsibilities

Methodology Definition

- Support for multiple initiatives and regulations in parallel
- Methodology model builder (likelihood, impact, risk and control categories, risk levels, etc)
- Risk, Control, Action libraries

Reports and Analysis

- Methodology overview reports
- Risk assessment reports
- Mitigation actions monitoring reports
- etc

Unified Actions Management

- Enterprise portal user interface for unified actions management
- Client user interface
- User dashboard view
- Scheduled and ad hoc alerts

Environment Definition

- Organizational structure
- Functional areas
- Functional activities
- Assets
- Third parties, etc.

Access and Authorization

- Comprehensive access control
- Role and user authorizations based
- Active directory integration

The RCMS Application: Key Modules Details

- The **Environment Definition** module allows users to define the scope of the assessment and develop the framework to which the scope applies. This includes documenting the relevant value chain or organizational structure, the associated functional areas, departments, functional activities, business processes, the associated owners, information systems, products / services, procedures, buildings and other key assets. This can apply to an organization, a department or a process / service.

- The **Methodology Definition** module allows users to dynamically define the approach to be utilized to perform an assessment and the relationship between impact, likelihood and risk. This module allows for custom and dynamic definition of impact levels, likelihood levels, multiple risk profiles, risk categories / subcategories, control categories / subcategories, risk library, dynamic risk level definition, etc.

- The **Risk Management Module** covers the *Strategic Risk Assessment* and the *Detailed Risk Assessment* functionality. The Strategic Risk Assessment addresses the organization at the strategic level and applies a top down approach to set the strategic risk focus of the organization. In turn it generates a strategic approach in performing more detailed risk management activities. This determines which areas (functional activities, departments, processes, etc) the Detailed Risk Assessment will address. The Detailed Risk Assessment constructs and executes an appropriate risk-library-driven assessment for the environment under consideration, if required, to initiate and facilitate the assessment. The application is a dynamic platform that can also be used to facilitate a Self Assessment process by adding risk entries at any time. The triggers can be documented and developed into specific risks that can be used in the future to facilitate a structured assessment process. Furthermore, the specific controls that exist are documented and the mitigation actions and their status and implementation plan are identified, documented and monitored.

The RCMS Application: Key Modules Details

- The **Compliance Management** module allows users to register and list all compliance requirements either due to a regulation or due to an audit or other source, by each source (e.g. internal audit, security requirements, third party audit, pci audit, pen test, etc) of interest to the organization. The module allows users to create a source (e.g. audit by an external entity – such as PCI, Internal Audit or a regulatory compliance requirement) and then add the compliance requirements / findings that need to be managed, followed up etc. Each requirement is registered and the defined actions associated to the fulfillment of the requirement / finding are registered and linked. The actions can be monitored also via the unified Actions Monitoring module. Requirements and findings are able to be linked to identified risks registered via the Risk Management module.
- The **Incident Management** module allows users to register, analyze and manage identified incidents / events. Captured data includes the discovery date, occurrence date, identified by , title (brief description of event), description (more extensive description of event), event type, the department/business line to which the event relates, the cause of the event, mitigation actions set / taken by the organization to manage and mitigate the event, recovery status, near miss, financial impact amount, recovery amount, insurance amount, net loss amount post recovery and insurance cover, etc. The mitigation actions can be monitored also via the unified Actions Monitoring module.

The RCMS Application: Key Modules Details

- The **Unified Actions Monitoring** module includes all actions to be monitored form the Risk Management, Compliance Management and Incident Management modules. This includes the functionality that gives the option to assign and follow up tasks related to risk / incidents and findings with automated email notifications sent to employees and their supervisors for pending and overdue observations and chronological history of the responses received, so as to track actions. In addition a web based interface can be provided as an optional item to serve all users that require only access to the actions monitoring functionality to manage and edit actions relevant to each user.
- The **Report Generator** is used to produce and present the results from the completed assessments and the status of ongoing activities (e.g. mitigation actions completion level). The results are suitable for interpretation by both technical and non-technical management and are in the form of a professional business document. As an example, a number of reports are provided including, but not limited to:
  - Overview of the environment under assessment;
  - Asset information report;
  - Overview of the methodology parameters followed;
  - Comprehensive risk assessment report;
  - Risk matrices;
  - Risk dashboards; and
  - Mitigation action reports.

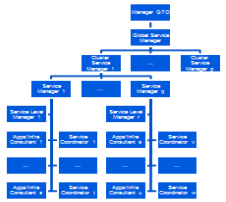
03.

The integrated functionality

The RCMS Core Components

Risk Management

Compliance Management



Organizational Structure

Common Data and Methodology

Incident Management

Unified Monitoring

The RCMS Functionality Modules

- Maintenance (Universe Definition)
- Risk & Compliance Functionality Modules
- Access, Authorization & Collaboration

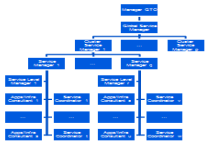
!

The Organizational Structure, Environment Definition, Methodology Definition modules must be configured prior to rolling out the solution

The Series of Events

DEFINE UNIVERSE & ROLES

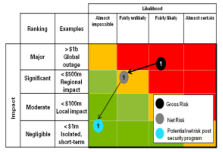
- Roles & Authorizations



- Organizational Structure

- Assets
- Third Parties
- Etc

CONFIGURE METHODOLOGY



- Categories & Types
- Levels
- Ratings
- Risk Matrix
- Other Parameters

- Template Libraries

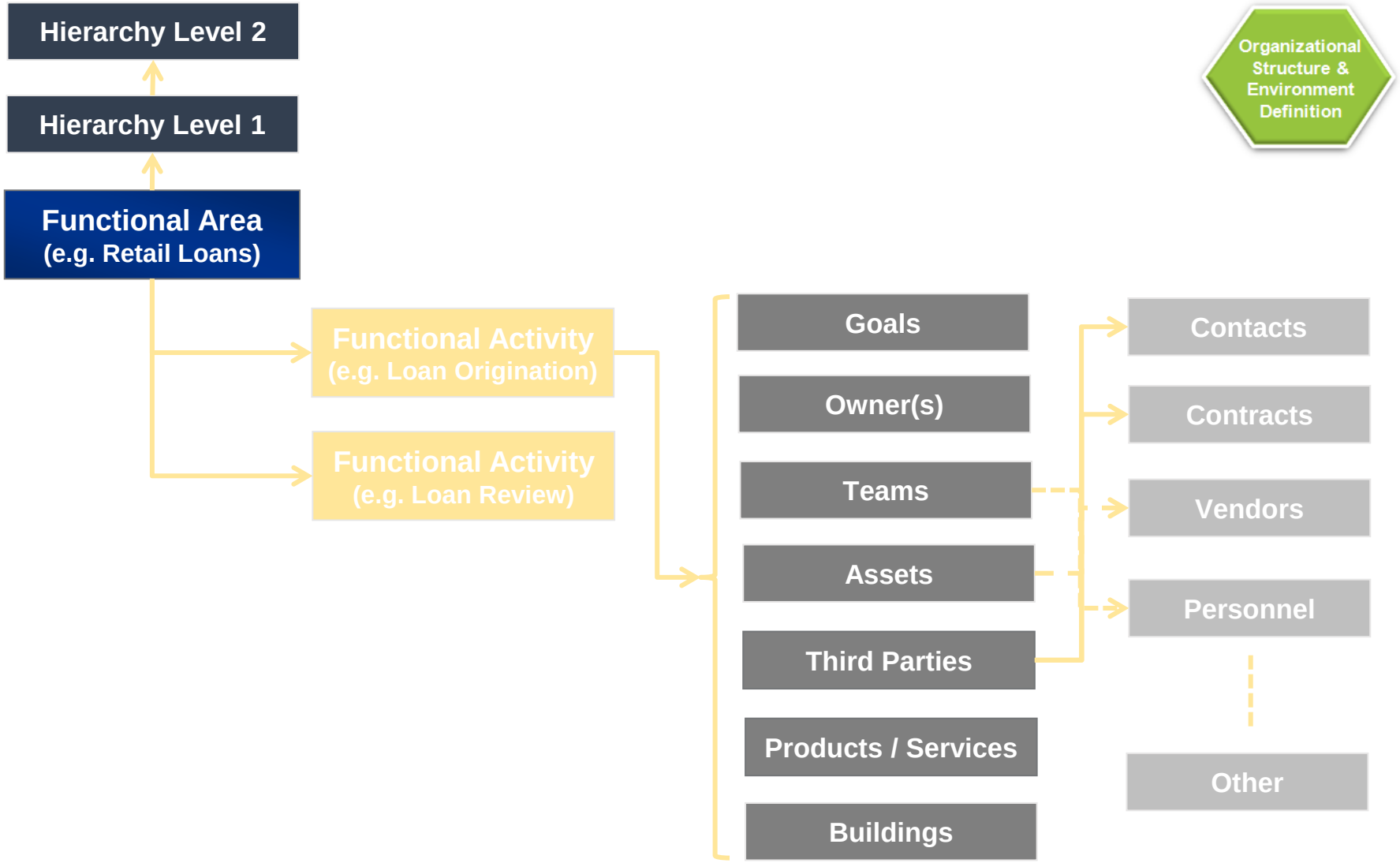
EXECUTE

RCMS PLATFORM

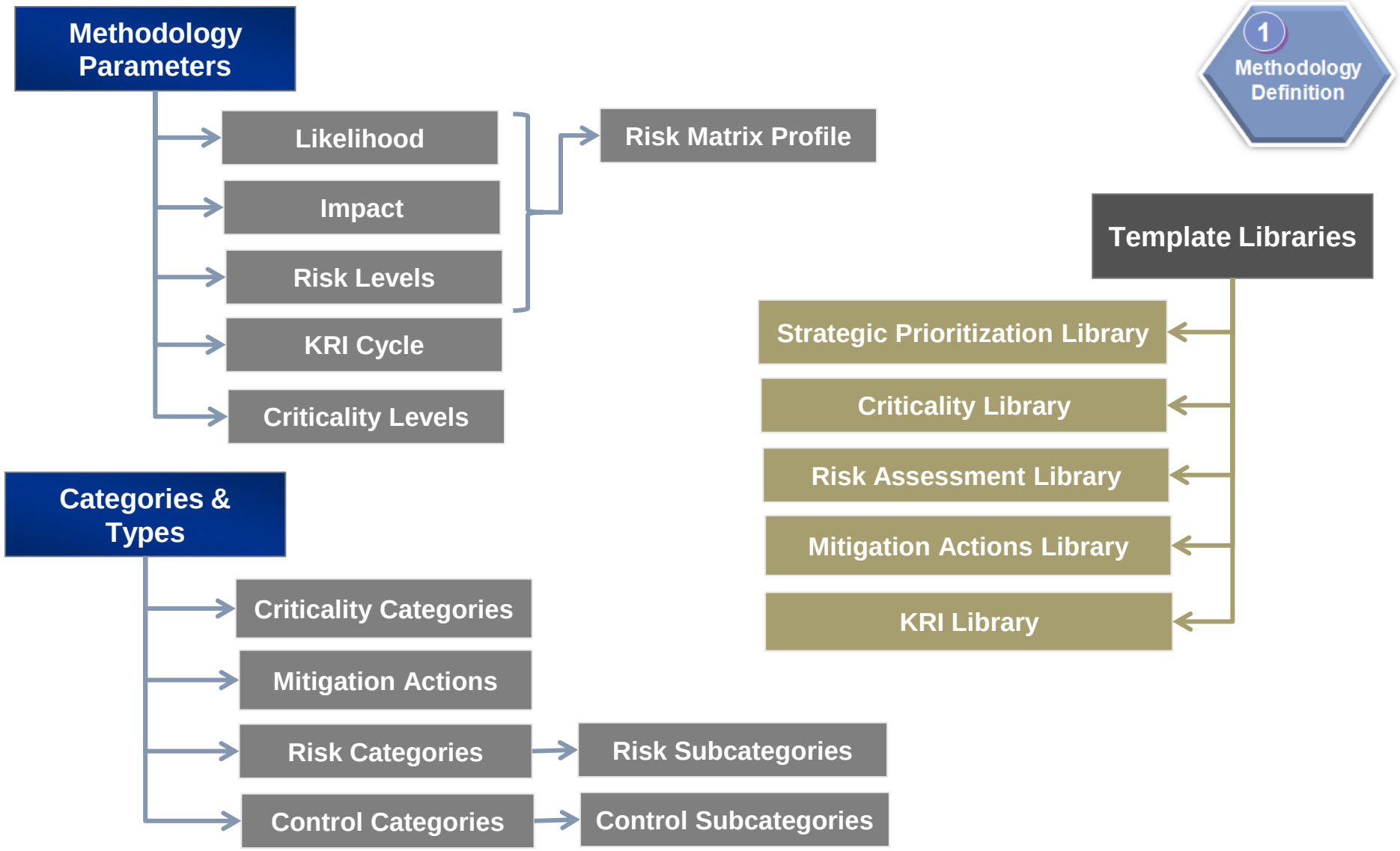
- Strategic Assessment
- Criticality Assessment
- Risk Assessment
- Compliance Management
- Incident Management
- Unified Monitoring
- Reporting

Continuous cycle

Organizational Structure & Environment definition



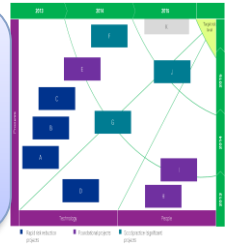
Methodology Definition



Risk Management Cycle

- Update risk exposure
- Monitor Key Risk Indicators (KRI)
- Capture Incidents and Losses

- Align risk approach to organization's structure
- Define risk assessment model
- Define risk relevant business activities



Risk Plan

Risk Monitor

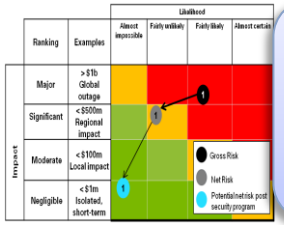
Risk Identify

Risk Mitigate

Risk Analyze

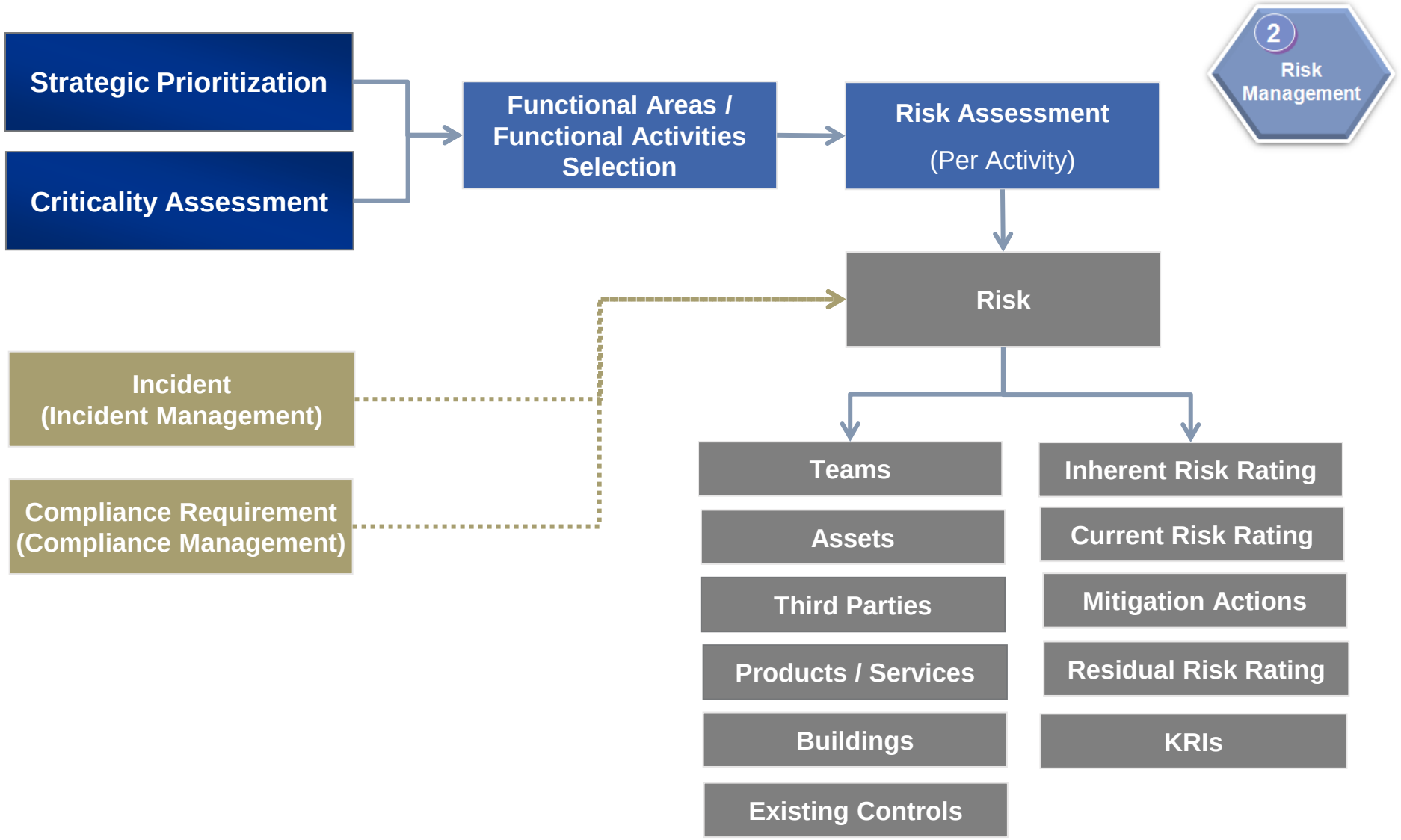
- Identify risks and opportunities
- Risk categorization
- Key Risk Indicators

- Preventive and corrective actions
- Assessed residual risk
- Track Mitigation actions Status

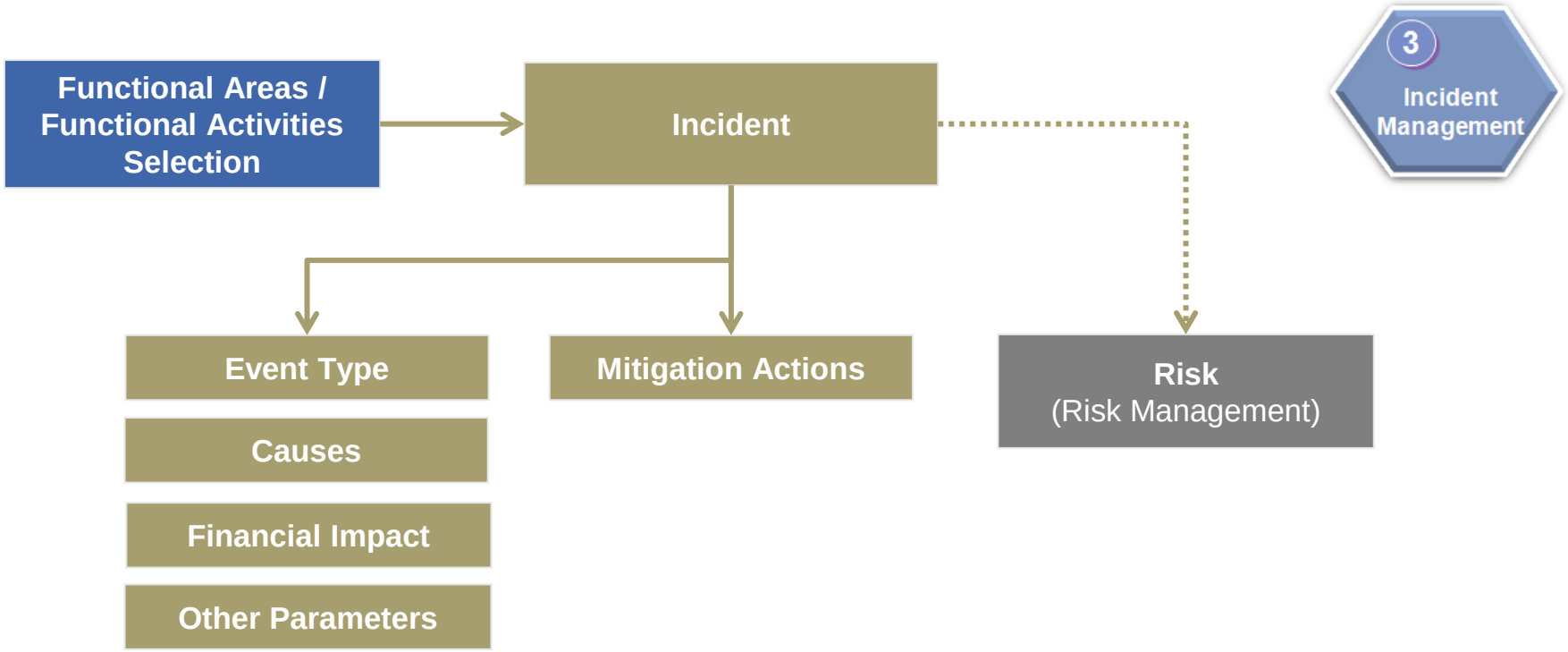


- Impact analysis
- Likelihood analysis
- Event type analysis
- Risk levels / profiles
- Heat map
- Control analysis

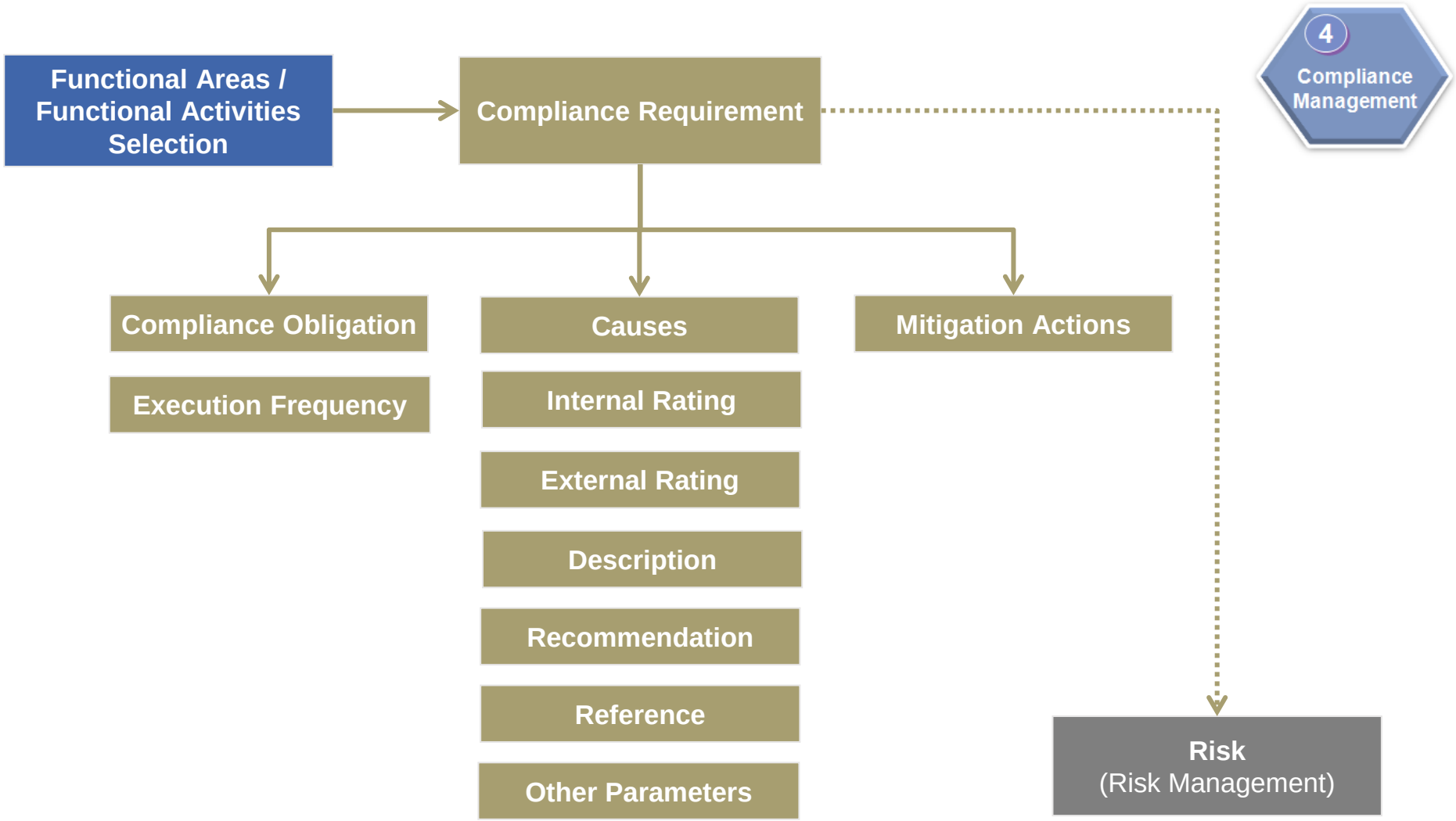
Risk Management – Series of Events



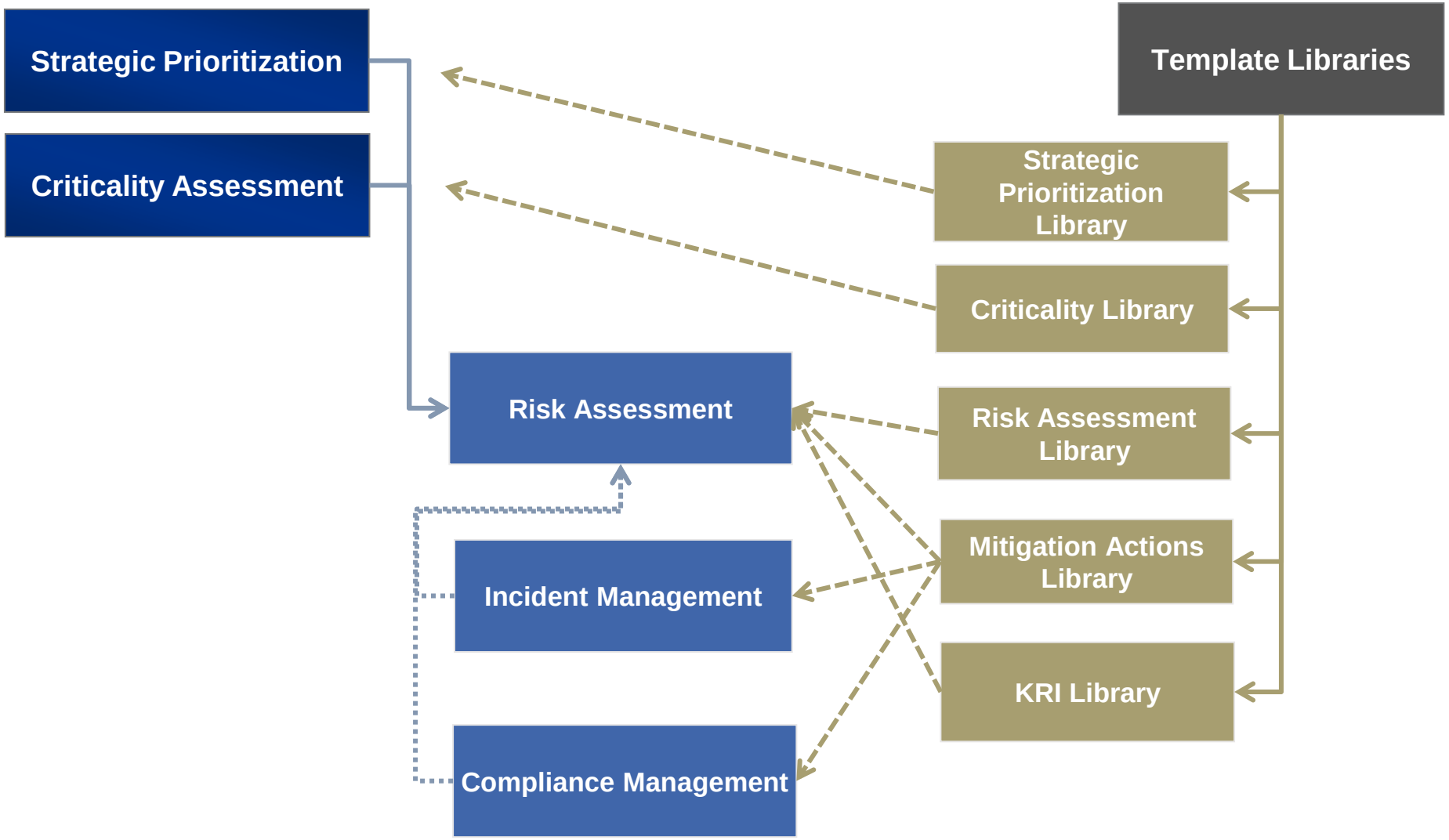
Incident Management



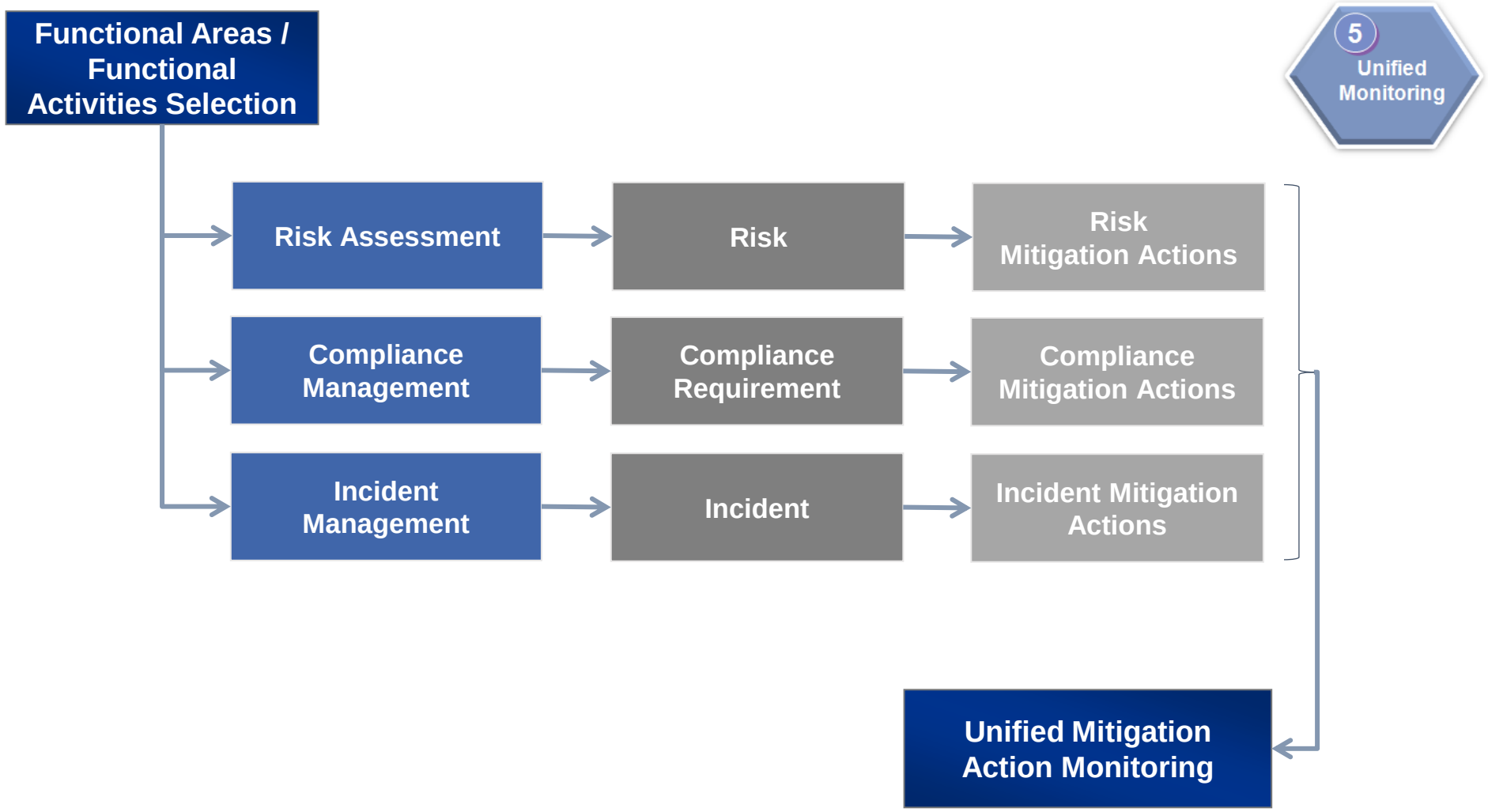
Compliance Management



Use of Template Libraries



Unified Monitoring



Reporting Analysis

- Predefined Reports
- Custom Reports
- Ad-Hoc Reports

03.

Example Project Plan

Phases and Activities (Note: Example does not include advisory services)

Phases	Activities (estimated elapsed period)
1 Provision of Software and Installation	■ Kickoff meeting ■ System installation (2 days) ■ Gathering of data parameters required (1 week) ■ Loading of data in system database (3 days)
2 Configuration of Solution	■ Review of data parameters and approval (2 days) ■ Integration (2 days) ■ Key Users set up (1 day) ■ Configuration of Organizational Structure (2 days) ■ Configuration of methodology (3 days) ■ Review of set up and approval (2 days)
3 Key User Training	■ Key user training session (1 day)
4 Post Implementation Support	■ Standard support and maintenance ■ Advisory support (optional)

Visit our website to check out our Compliance Solutions

CHRISTOS TTINIOZOU
MANAGING DIRECTOR

Phone: +35799648913
Email: cttiniozou@i-spiral.com