Deloitte.

Risk and Controls Centre of Excellence

Next-gen internal controls and compliance organisation

Introduction

The current global environment is characterised by change, uncertainty, and disruptive innovation. These changes are fundamentally transforming organisations and affecting the world of Internal Controls (ICs).

Given the cost pressure, increased scrutiny from regulators, and an unpredictable business environment, organisations are considering a Risk and Controls Centre of Excellence (RCCoE) to centralise and support risk management activities while optimising cost.

What is a Risk and Controls Centre of Excellence (RCCoE)?

Risk and Controls Center of Excellence is a next-gen centralised IC and compliance organisation that helps evolve from a traditional risk management approach (which was manual and reactive) to a more advanced set-up (which is automated, predictive, and near real time).

It is established with an objective to support regulatory and operational compliance activities across both the process and IT domains.

The RCCoE is owned by the second line of defence. These centres follow a modular approach with a plug-and-play architecture, which enables them to support the first and third lines of defence.

The set-up is technology agnostic and can be integrated with any commonly used Governance, Risk, and Compliance (GRC) platform.

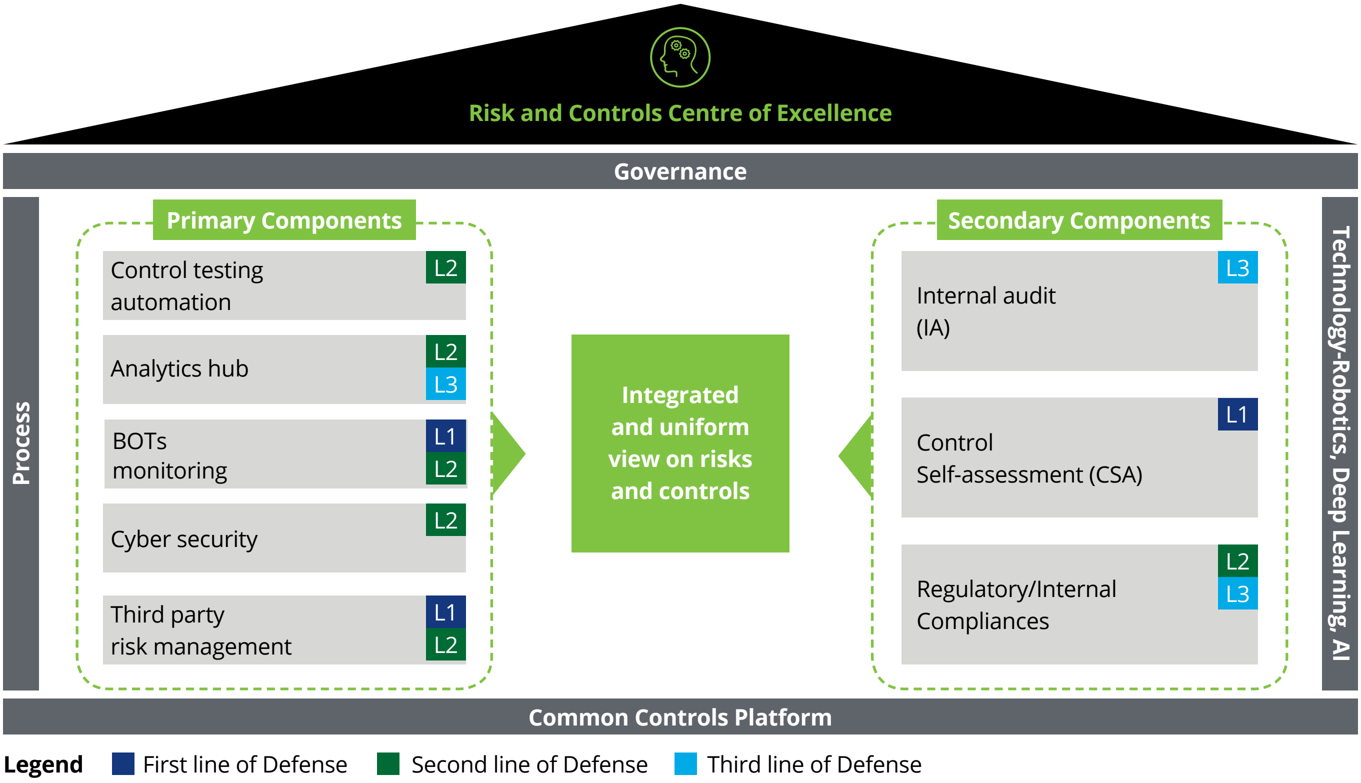
A robust governance framework with tightly defined scope, clear communication and interaction model ensures hassle-free operations.

Additionally, technological accelerators, such as robotics, machine learning, deep learning, and artificial intelligence, allow predictive analysis for risk management.

Features of a Risk and Controls Centre of Excellence

- Control testing automation
- Modular set-up, with plug and play architecture
- Supports all three lines of defence
- Technology agnostic integrated platform
- Predictive and near real-time monitoring

A typical RCCoE and its components are shown below.


Risk and Controls Centre of Excellence
Governance
Process
Primary Components
Control testing automation L2
Analytics hub L2 L3
BOTs monitoring L1 L2
Cyber security L2
Third party risk management L1 L2
Integrated and uniform view on risks and controls
Secondary Components
Internal audit (IA) L3
Control Self-assessment (CSA) L1
Regulatory/Internal Compliances L2 L3
Technology-Robotics, Deep Learning, AI
Common Controls Platform
Legend
First line of Defense
Second line of Defense
Third line of Defense

The components of an RCCoE are bifurcated into primary and secondary. As the RCCoE is owned by the second line of defence, activities that pertain to management assurance are primary components and those performed by the first or third lines of defence are secondary components which can be included as required. Given the independence requirements, a co-sourcing operating model is preferred for activities managed by the third line of defence.

Predictive, recurring, and well-documented activities lend themselves more naturally to this set-up. Therefore, such activities take precedence during the process of transitioning to this organisation.

The results and/or status of all activities performed in the RCCoE can be reviewed through near real-time power BI or Tableau dashboards. Reports are generated in the central RCCoE hub.

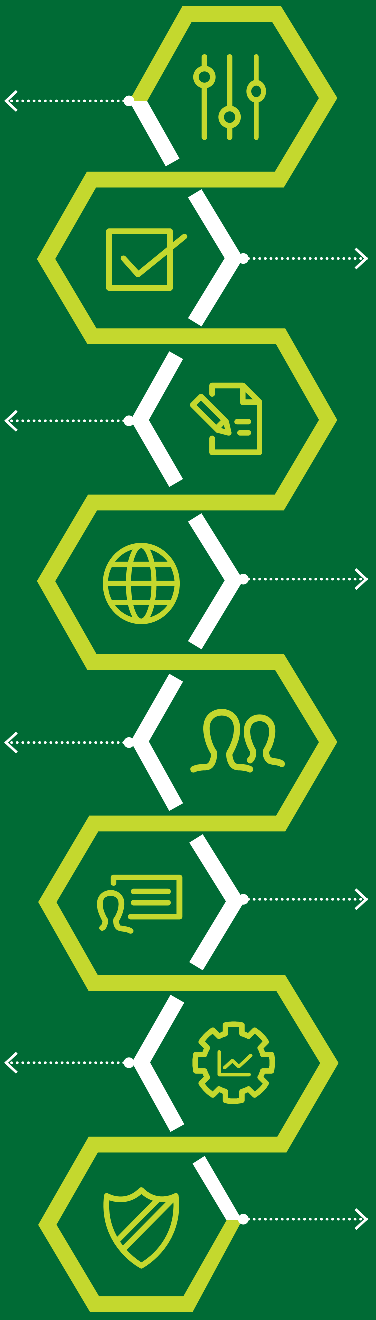
The primary components and examples of activities that can be managed from an RCCoE set-up are explained in the following section.

Risk and Control CoE Components

	Component description	Examples of activities performed
Control testing automation	Use of Robotics Process Automation (RPA) to manage administrative and core activities involved in the review of operational and ICs over financial reporting	• Administrative/Project management activities: Creation of the testing calendar/schedule testing, management of document/information request, and creation of audit reports in a standard template • Core testing activities: Execution of IT general controls testing at the application, database, and operating system layers per a defined test plan
Analytics hub	Risk-based and predictive control analytics to interpret data and gain insights with near real-time dashboards, reports, and exception monitoring capability	• Impact analysis of segregation of duty to determine if conflicting access has been misused • Review of change management controls to verify that all changes are approved and adequately tested before going live
Bots monitoring	Assurance/monitoring performance of operational and IC activities where RPA is deployed	• Review of close activities performed through RPA for comprehensiveness and accuracy • Review of access rights revocation scheduled through RPA
Cyber security	Design, implementation, and management of cyber security control measures	• Vulnerability assessment, penetration testing, and application security review
Third party risk management	Services such as SOC reports, HITRUST CSF certification, compliance reviews, End to End Vendor Management, and IT compliance reviews	• Contract compliance review to check adherence to standard terms and conditions • SOC report evaluation and automation • Vendor screening

Key considerations while setting up a RCCoE

Organisations must keep in mind the below considerations while implementing a RCCoE. These considerations will ensure a structured, realistic, and phased approach during the set-up.



Process and controls

- Create a standardised common control framework (only limited variations due to unavoidable business and regional nuances should be permitted)
- Check consistency in rigor around Internal control activities

Business acceptance

- Ensure management buy-in to new delivery models
- Manage local regulatory requirements
- Consider country specific language requirements

Business case

- Identify any inaccuracy of estimates (tangible/intangible)
- Evaluate the financial model to project return on investment (ROI)
- Check for realisation of the business case

Global capability centres

- Expand the scope and capabilities
- Ensure availability of the right skillset and talent management

Change management

- Create and implement initiatives to overcome resistance to change, conflicts, and knowledge transfer complexities

Migration approach

- Evaluate strategy (lift and shift versus transform and shift)
- Create service-level agreements
- Plan transition and ramp-up
- Clarify ownership with roles and responsibilities

ERP environment

- Standardise the ERP landscape
- Ensure optimal use of standard ERP functionality for automation of manual controls

Awareness and ownership of ICs

- Specify control ownership, measure results, and undertake remediation as required
- Ensure no dilution of control ownership

Key benefits of an RCCoE

The foremost benefit of an RCCoE is that it provides a single consolidated view of the organisation's control health. Furthermore, consolidation helps build a business case to invest in a technological platform and opens up the possibility of automation of risk management activities. Other benefits of RCCoE are as follows:

Enhances control environment, ownership, and oversight

- Establishes a centralised operating model to formalise risk and control practices across functions, and define control ownership
- Creates a single source of truth, drives standardisation, and helps replicate best practices across the globe
- Uses tools and technology to facilitate the creation of advanced dashboards for near real-time reporting on control health and remediation status, and move swiftly from data-to-insights-to-action.
- Improves control effectiveness as automation decreases errors and helps maintain a better audit trail
- Builds capability to extend the scope and review larger sample sizes through analytics, thereby improves control effectiveness at no additional cost

Efficient resource utilisation

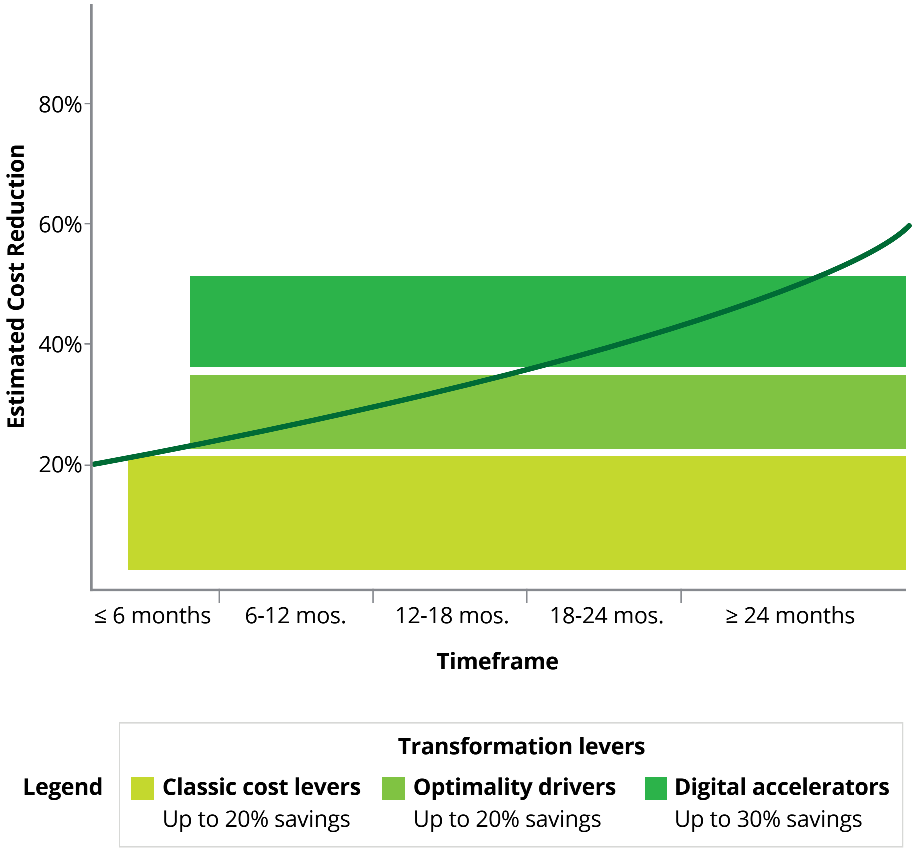
- Improves resource alignment to focus on the core business
- Helps improve productivity through "right sizing" and "right shoring" of the controls and compliance team
- Helps overcome skillset challenges and manage expectations

Optimise cost

- Eliminates functional overlaps among risk management activities
- Helps realise economies of scale on account of the centralisation of scope
- Supports labour arbitrage if the set-up is in low cost geographies
- Provides flexibility to scale up/down to manage fluctuating volumes

Further in terms of cost optimisation, below is an illustration suggesting the indicative roadmap of percentage cost reduction over a two-year time horizon. The actual savings will vary depending on the current state and maturity of the internal control organisation.

Illustration: Estimated savings through RCCoE



Conclusion

While the finance and accounting functions, and IT organisations have been using a centralised operating model over the years, IC organisations are now more actively adopting this set-up.

The approach to set-up a RCCoE will include a assess, design, implement, run, and operate phase. A well-designed and focused RCCoE addresses a wide-risk universe and provides a holistic view of the global controls posture. It improves governance while optimizing cost and resources. It transforms risk management practices and internal controls organisations thereby driving impact.

Contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Peeyush Vaish
Partner, Risk Advisory
Deloitte India
peeyushvaish@deloitte.com

Afshan Khayum
Executive Director, Risk Advisory
Deloitte India
akhayum@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.