

The Future of IT Internal Controls – Automation: A Game Changer

January 2018

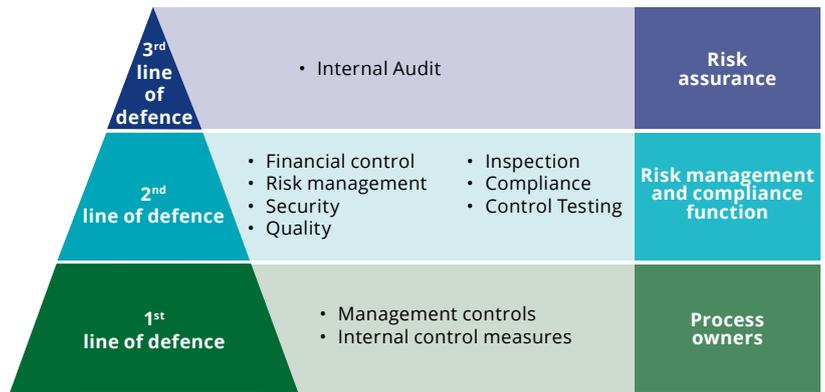
Contents

Introduction	01
Future Operating Models for Managing Internal Controls	02
Summary	07

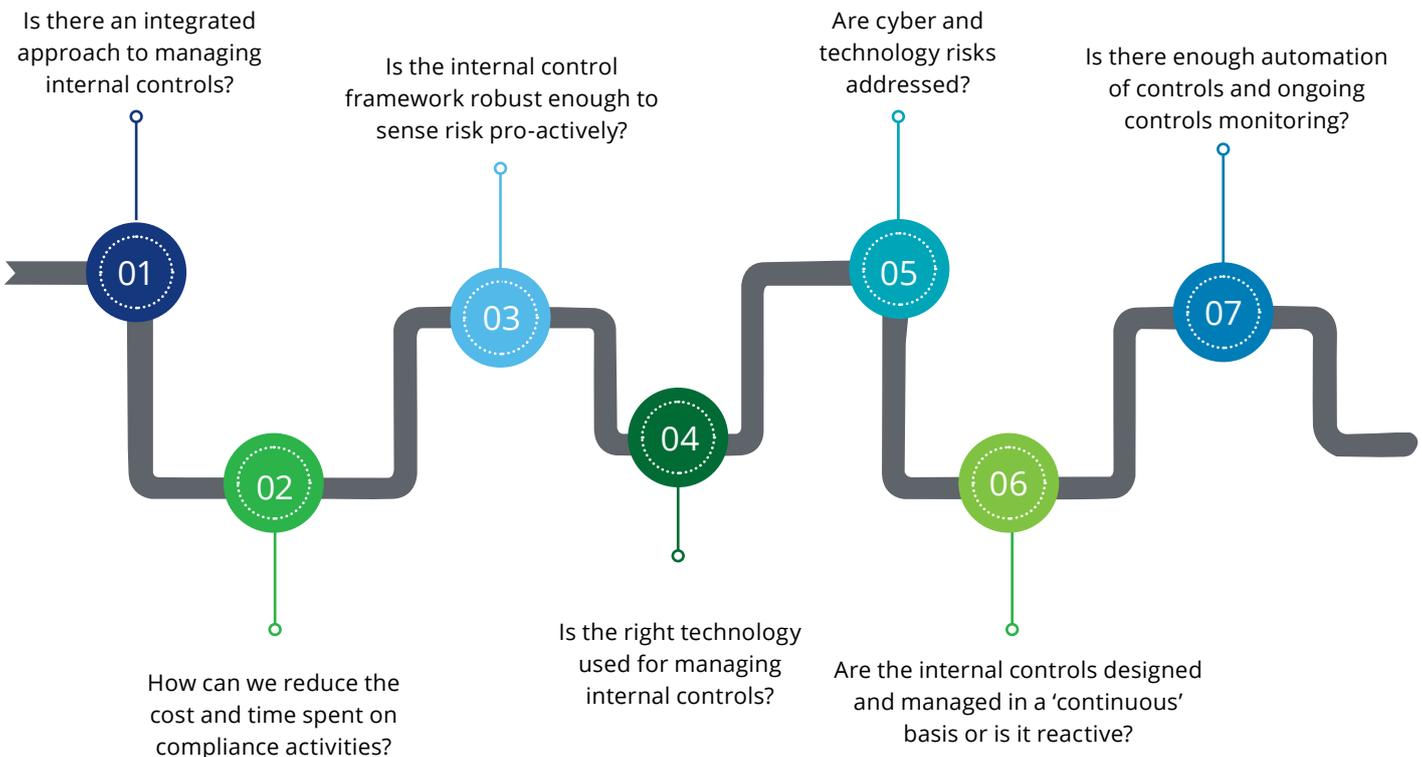
Introduction

Internal controls continue to be a key focus area for companies, regulators and shareholders. Compliance costs are increasing in organizations. Companies are using the three lines of defense to manage internal controls:

- First line of defense: Operational Management
- Second line of defense: Risk management and compliance/controllership function
- Third line of defense: Internal Audit.



Despite three lines of defense on Internal Controls, the Senior Management are faced with questions and challenges:



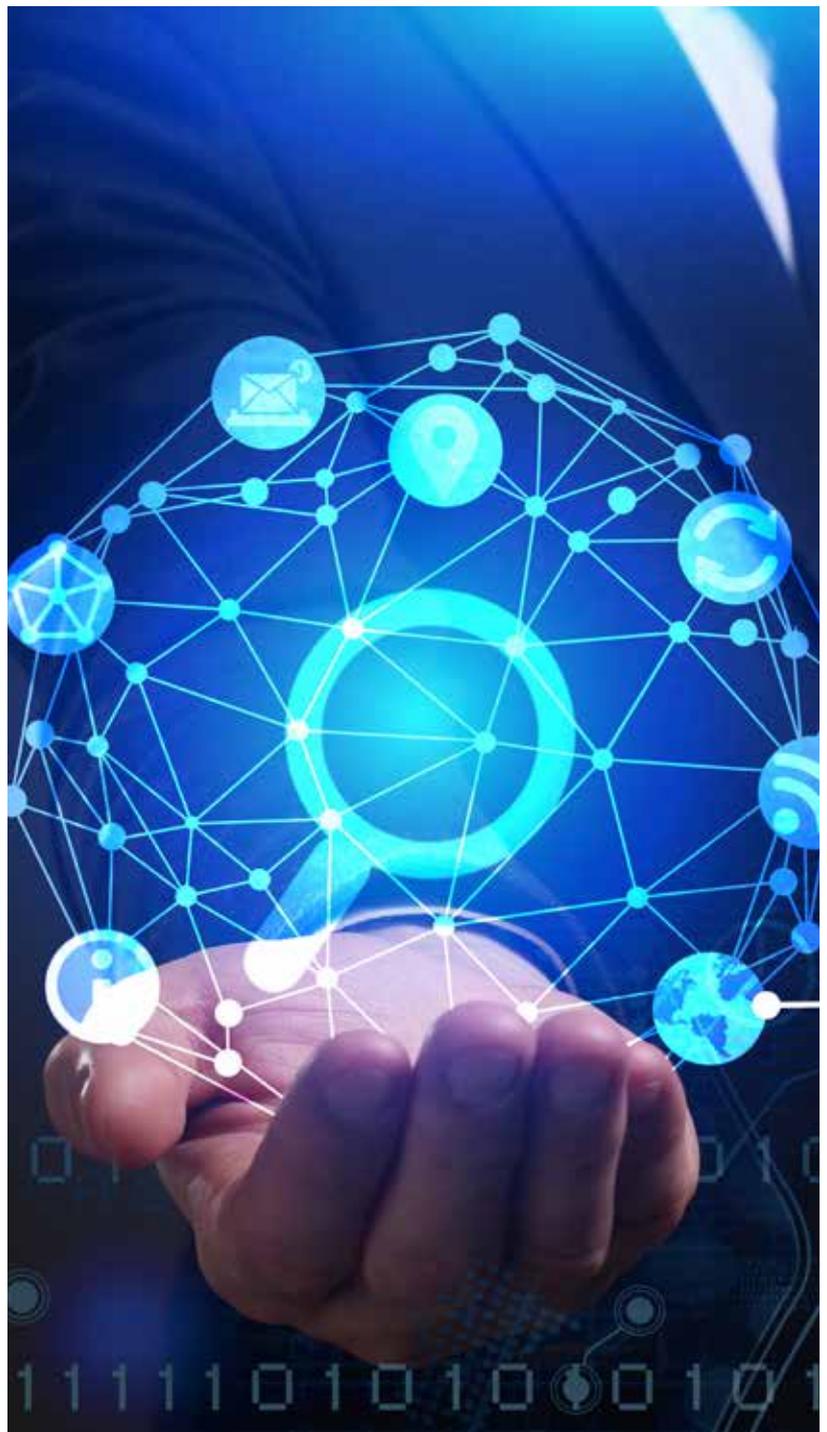
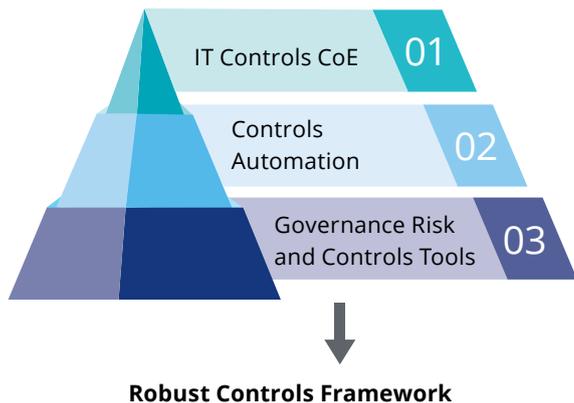
In the following sections we have outlined an approach that can help in addressing the above challenges and helping organization having a Robust Controls Framework.

Future Operating Models for Managing Internal Controls

Global organizations today are adopting certain operating models to bring in efficiency and perform ongoing monitoring of internal controls. There are number of approaches/ options that organizations today have, to build a Robust controls Framework, this includes but not restricted to:

- Setting up a IT Controls Center of Excellence (CoE) for managing controls
- Having an Integrated controls framework
- Rationalization of controls
- Implementation of GRC tools to manage and monitor controls
- Implement Continuous controls monitoring (CCM) solutions
- Centralization of testing of controls/ Outsourcing the activities of testing of controls
- Using analytics for testing of controls
- Implementation of Robotic process automation for controls testing etc

In this thoughtpaper, we have articulated 3 key priorities as shown below that organizations should focus.



1. IT Controls Center of Excellence (CoE):

Companies today are setting up IT Controls Center of Excellence to manage internal controls. The internal controls that can be managed centrally are shifted to the IT Controls Center of Excellence, which will be an independent function. However they will be working in an integrated manner with the IT operations teams. The IT Controls Center of Excellence will be working as a Second line of defense.

The IT Controls Center of Excellence will be involved and they will provide support in:

- Assist in performing Risk Assessments on the IT applications and supporting infrastructure.
- Assist in scoping discussions (e.g. SoX scoping) with External audits
- Assist in conducting trainings to the business/ operations team on compliance/controls related requirements
- Perform Design and implementation review of controls and also perform Operating effectiveness testing of controls. This includes automated controls, Master Data related controls, IT General Computer Controls.
- Monitoring controls on a continuous basis
- Assist in co-ordination of the external audits/compliance requirements
- Assist in remediation of Audit findings from controls perspective.

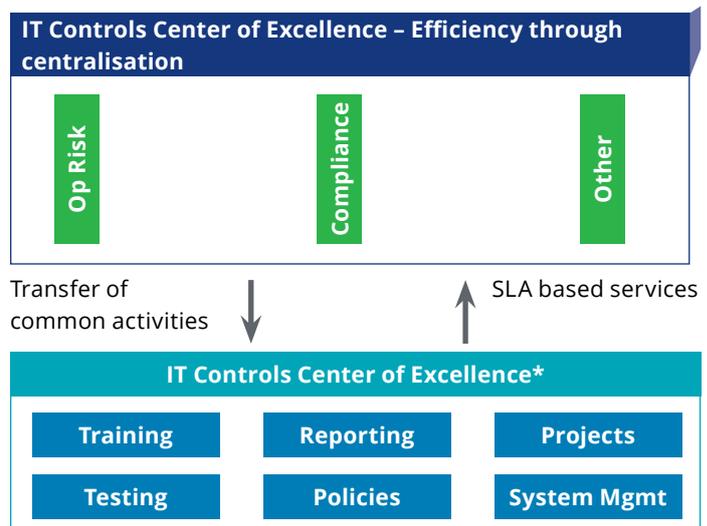
This model brings in scalability and agility as it helps in rationalizing, automating and standardize the process, controls and data to a central location so that any changes in any of the above elements could be addressed in an easier way. In an outsourcing model the controls

are tested and monitored by outsourced service providers.

Some of the unique feature of this model includes:

- Centralize activities common to control functions in a IT Controls Center of Excellence. This helps in building consistency in the operations of controls
- Retain specialist activities within control functions
- Relationship governed by SLA ensures the accountability of the Controls Shared Services.

The IT Controls Center of Excellence can be either managed internally or externally by Outsourced Service Providers. Service Level Agreements are signed between the IT Controls Center of Excellence (either Internal or outsourced) and business.



2. Controls Automation:

Controls automation is a key aspect of managing internal controls. It brings down the cost of compliance. The controls automation has two parts to it:

- **Automation of existing Manual Controls:** Control automation is brought about in terms of configuration changes, code changes or by using some tools such as identify management systems , GRC systems etc. Some examples of controls automation include the following:
 - Workflows could be enabled in the system to create user accounts based on the approvals as per the authority matrices. A system check for the SOD scenario can also be enabled with the user provisioning system
 - An identity access management system can automate the access revocation based on the last working day. This would be very valuable for the firm considering most of the big organizations have multiple applications and timely removal of access is area of concern.
 - Changes to any system can be routed through a system work flow which will ensure that appropriate approvals and testing is done prior to implementing the change.
 - Review of logs such as user activity log and admin activity log to keep a check on certain unauthorized transactions
 - Granting admin access or privileges can also be automated by enabling workflows for approvals and also a validity period for these elevated access in the system.
- **Automation of Controls Testing**

Testing of controls can be automated to bring in more efficiencies. This includes implementation of automated scripts for performance of the controls testing, implementation of RPA solutions, using analytics etc.

Most of the organizations use scripts based controls testing approaches where a script is run on the production environment of a system to download certain tables and structures and algorithms are written to read these data dumps and give the users a readable file to analyse. A user intervention is mostly required in this scenario to analyse the data and classify the control to be effective or ineffective.

Robotic process automation (RPA) can also be deployed for the same. RPA is the application of technology to perform rule based tasks and interface with existing applications in order to complete assigned tasks. Testing of some of the controls can be automated from start to end. There are multiple tools for RPA in the market such as UiPath, Automation Anywhere and Blueprism.



Some of the cases where RPA can be used in control testing are:

- BOT's (algorithms) can be implemented to login and download all the changes on a system during a period and then reconcile it with another report downloaded from a ticketing system which captures the approvals. A direct exception report can be created for 100 percent of changes where there are no approvals or where approvals are taken post implementation of changes.
 - Similar algorithms can also be created to check for exceptions in the case of user access creations. It does not matter whether approvals are taken in hard copy forms of by means of E mails, technology such as OCR (Optical character recognition) and AI (Artificial intelligence) can be used for this.
 - Status of default user account control can also be tested using RPA. This can be end to end as in it can also fill in documentation templates for the controls tested and even store in document repository for further review.
 - RPA can also be used in testing segregation of duties / environments controls.
- **Automation of Controls Monitoring:**

The third part of controls automation, is to implement solutions that can help in monitoring of controls. Some examples of automation of controls monitoring include:

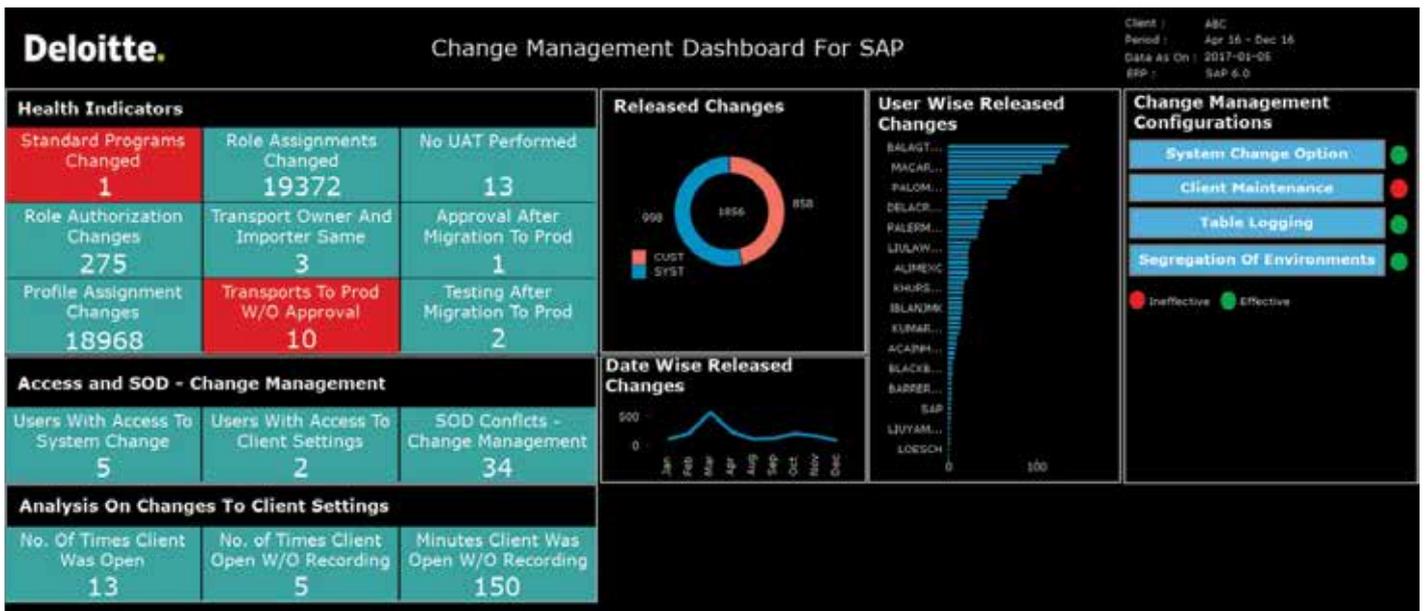
 - Configuration controls: Dynamic dashboards can be built to check whether the configuration behind a control is set as per the recommended settings and also to see how many times during the period of review, this has been changed. Alerts could be

- also enabled to be sent to control owner once these settings are changed. E.g. Client settings (SCC4) and Global setting in SAP (SE06).
- Exception reports: Exception reports are built using a predefined rule. This predefined rule is designed based on some specific business or audit requirements. This could be simply as identifying emergency changes from the list of all changes or to identify cases where user access is created before the approval.
- Actual usage conflicts of Segregation of Duties: After identifying the access level conflicts existing in the system, it is imperative to know whether this conflicting access has been misused at all. This helps to understand the impact of these conflicts better.

- Access related controls: Analytics could be applied to monitor the user access controls such as approved user creation, timely revocation of access for exit and transfers, access reviews admin activity reviews and default users.
- Change management controls : A continuous monitoring can be established to see if all the changes are approved and adequately tested before moving it into production, to see if there is significantly higher number of emergency changes , if initiator and approvers are the same ,

The continuous controls monitoring tools can help in achieving automation through controls monitoring.

Illustrative dashboards that CCM solution can present is displayed below





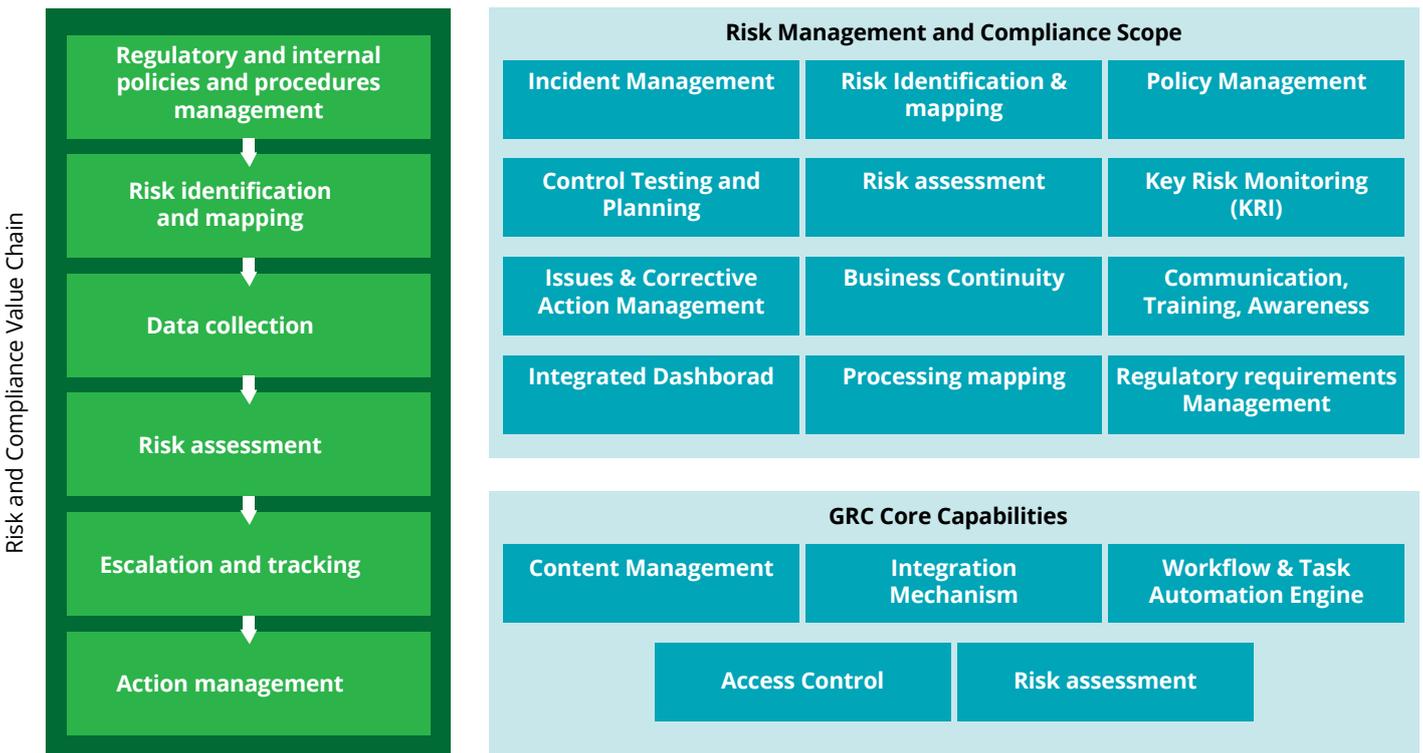
3. Implementation /enhancing the use of GRC tools:

Many organizations today have implemented or in the process of evaluation of Governance Risk and Controls solutions. GRC solutions can bring in consistency and help to sustain Internal Controls framework from IT perspective. Some of the examples on using of GRC tools from IT Controls framework include:

- **Risk Assessments:** GRC tools can help in performing Risk assessments based on category of risk for an application. Further the GRC tools have inbuilt controls library that can be used /customized for implementation of controls based on risks.
- **Integrated controls framework:** GRC tools help in implementing an integrated controls framework. The various controls requirements (such as SOX, PCI DSS, ISO 27001) can be combined and rationalized into a single framework
- **Documentation:** GRC tool will act as a repository for all the documentation related to internal controls.
- **Issue tracking:** All the controls related failure can be monitored through the GRC tools. Monitoring of the issues and tracking of remediation will be done centrally through the tool.

GRC tools can be integrated to CCM solution, testing results can be stored in one place. GRC tool will act as enabler to bring in efficiency in the Controls Automation journey.

An overview of the GRC modules are listed below:



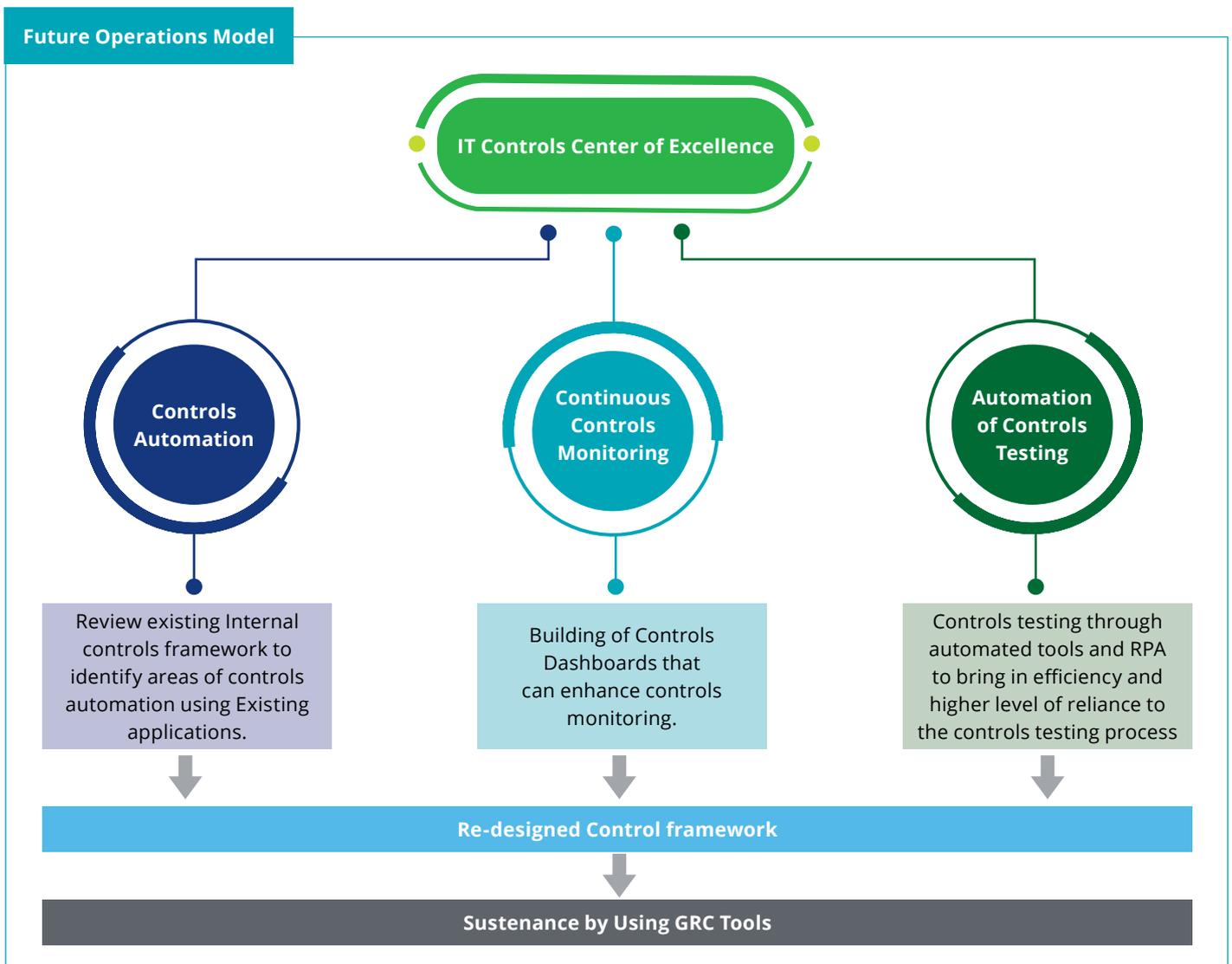
Summary



The key priorities/ focus areas will help organizations to achieve a sustainable Internal Controls framework.

A centralized setup in form of IT Controls Center of Excellence will bring in standardization of control definition, removal of duplication of controls overlap and duplication, bring in efficiency for testing and monitoring controls. The IT Controls Center of Excellence will work with the Business/ Operations (First layer of defense) in an integrated manner to ensure

controls definitions and implementations are consistent. The IT Controls Center of Excellence will drive in Controls Automation in terms of automation of manual controls, using RPA for controls testing, using analytics for testing of controls. Implementation of GRC tools or enhancing the GRC usage will be an enabler to the IT Controls Center of Excellence in building an Robust Internal Controls framework and mostly importantly to sustain the framework in an effective and efficient manner.



Key Contributor

Deepa Seshadri

Partner

deseshadri@deloitte.com

David George

Senior Manager

georged@deloitte.com

Contacts

To learn how an organization can optimize their Internal Controls Framework, please contact:

Ramu N

Partner

E-mail: ramun@deloitte.com

Kedar Sawale

Partner

ksawale@deloitte.com

Deepa Seshadri

Partner

deseshadri@deloitte.com



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.