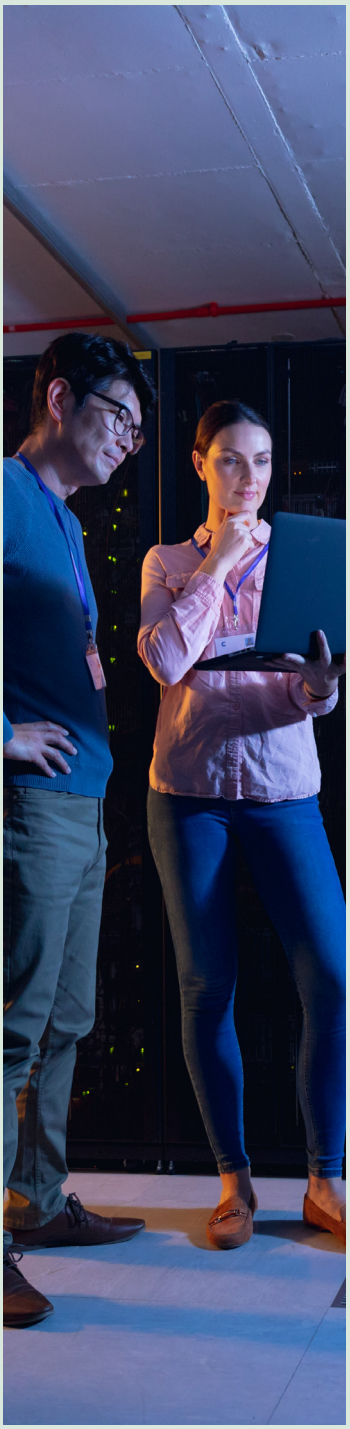
WHITE PAPER



A RISK-BASED CONTROL ASSESSMENT MATURITY MODEL

Infosys®
Navigate your next

Control maturity assessment is the first step toward operational excellence. Without an unbiased assessment of current processes, capabilities, and practices one cannot design the transformation for a realistic future state effectively and efficiently. Enterprise risk should be prioritized by organizations that believe in lean principles to improve productivity, reliability, and output quality. This approach will enable the enterprise stakeholders to evaluate the risk impact and manage overall control and oversight.

Maturity assessment is fundamental to assess various parameters of an organization before it matures towards continuous improvements. Following are some essential parameters measured by maturity assessment:

- Transformation potential
- Practiced lean culture
- Diversity in approaches, practices, and technologies

Yet, it is worthwhile to note that maturity assessment can run into unmanageable growth of controls and oversight. The number of assets monitored across the enterprise will overwhelm the monitoring teams. An asset type can be an organization, application, platform, web app, SaaS, mobile app, OT system, database, server, bot, communication room, archive room, third-party service provider, etc. As controls grow every year it is inevitable that the development teams will be bogged down under the pressure of monitoring and reporting them. To manage implementation work for the multiple controls, the maturity-based assessment must be designed in a way that it doesn't create any implementation bottleneck.

We believe to have found a solution to this chaos.

The risk-based control maturity approach: Five key principles

A good maturity assessment should follow 5 guiding principles – risk-based approach, independent evaluation, considering the current set of challenges, establishing success criteria, and identifying tangible improvement actions.

The guiding principles of risk-based control maturity assessment

Risk-based – The risk-based approach ensures that risk-reduction targets a clear alignment of goals and their tangible implementation. The controls are developed and monitored to identify the worst risks that threaten the most critical business areas. Organization's critical information assets (Crown Jewels), third parties that interface with the processes and the platforms on which it runs are often the ones that generate significant risks. Consequently, it is critical to examine the workflows and risks to which critical assets are susceptible. Identification of vulnerable workflows and processes will simplify risk identification. The risk register is used to manage the entire process of risk handling and assessment in the following ways:

- Map risks - basis severity and impact
- Improve the application of controls
- Improving the effectiveness of controls in reducing risks

Eventually based on the risk register- the areas where satisfactory control is present, the risk can be nullified. At this point, we can say that the risk-based approach has 'optimized' the risk landscape by linking them to the severity, controls, and the possibility of their occurrence.

Independent – It is extremely essential that the risk assessment is performed by an independent, unbiased entity, which is either part of the organization's COE or a third party. However, it is the responsibility of the independent team to not digress away from the day-to-day operations. Having strayed from the practicalities of the real world can give a rose-tinted view of the capabilities without offering any window on the challenges and issues. A face-to-face connect with the frontline team members is required to understand the processes and procedures enabling the work culture.

Challenges – The vulnerabilities existing in infrastructure and applications are the key challenges that need resolution as per the control framework accepted by the organization. It helps in identifying the improvement opportunities as well as underlining any hidden risks. The mindset of the frontline team members handling the asset is as important as the asset being examined. It is worthwhile to consider if self-disclosure should be encouraged to proactively identify and treat the deficiencies. This sheds light on how processes, assets, or services are constructed and utilized by the stakeholders. It gives a deep insight into the performance of the process or asset, proactiveness in identifying the gaps, and agility in closure. Challenging the current set of control designs for effectiveness, help identify problems before they occur versus handling their fallout.

Success Criteria – Define the success criteria versus checking whether the tools, processes, and procedures are in place. Reviews shouldn't be about whether best practices are in place. Reviews must question the suitability and applicability of controls. Targeted questions should be asked to determine the problem and the underlying root cause.

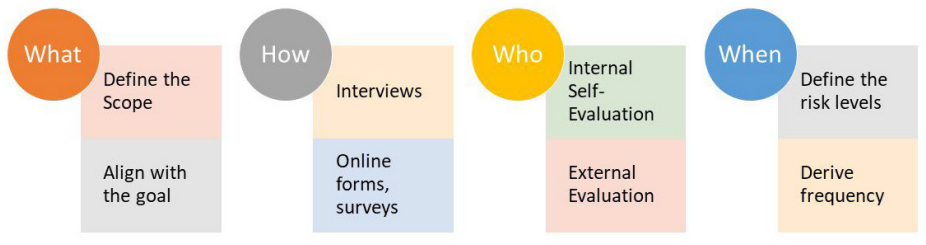
Improvement Actions – The end goal of an assessment should not be - pass or fail. A pass or fail is no indication of how the situation can improve. A useful assessment will help identify the cause of poor performance (from the success criteria) and suggest appropriate solutions. A good approach would be to define the RACI so that suggested improvements are owned and implemented.

We believe that this approach is effective as it keeps businesses informed of impending risks along with verifying the effectiveness of the controls implemented.

Assessment Model - Implementation Steps

An assessment of the 5 principles stated above should answer the following:

- Which entity/system needs to be assessed (The What)
- Process of assessment (The How)
- The individual/team responsible for the assessment (The Who)
- Assessment timelines (The When)



Implementation of the Assessment model – What, How, Who, When

What

Consider a comprehensive view of asset performance. Cover all the relevant categories based on risk classification, asset type – Applications, Infrastructure, Digital, Devices, Processes, Data Center, Communication room, Archive room, and Processes. Once the scope is set, the assessment will follow organizational policies, processes, procedures, and control register.

To evaluate asset performance, the assessment must align with the organizational goals and meaningful purpose. It is imperative to understand the ability of an asset to ensure that it delivers value efficiently and effectively.

How

Assessment should be based on interviews, evidence observations, online forms, and surveys. Objectivity and accuracy are key elements to obtaining an actionable implementation plan from identified risks/findings. Conducting a self-assessment and an external assessment led by independent evaluators triggers powerful discussions focusing on the differences. The insights obtained from this further help strengthen the control design.

Who

Experienced evaluators (internal or external), who have expertise of the business, controls, tools, and processes should perform the assessment.

When

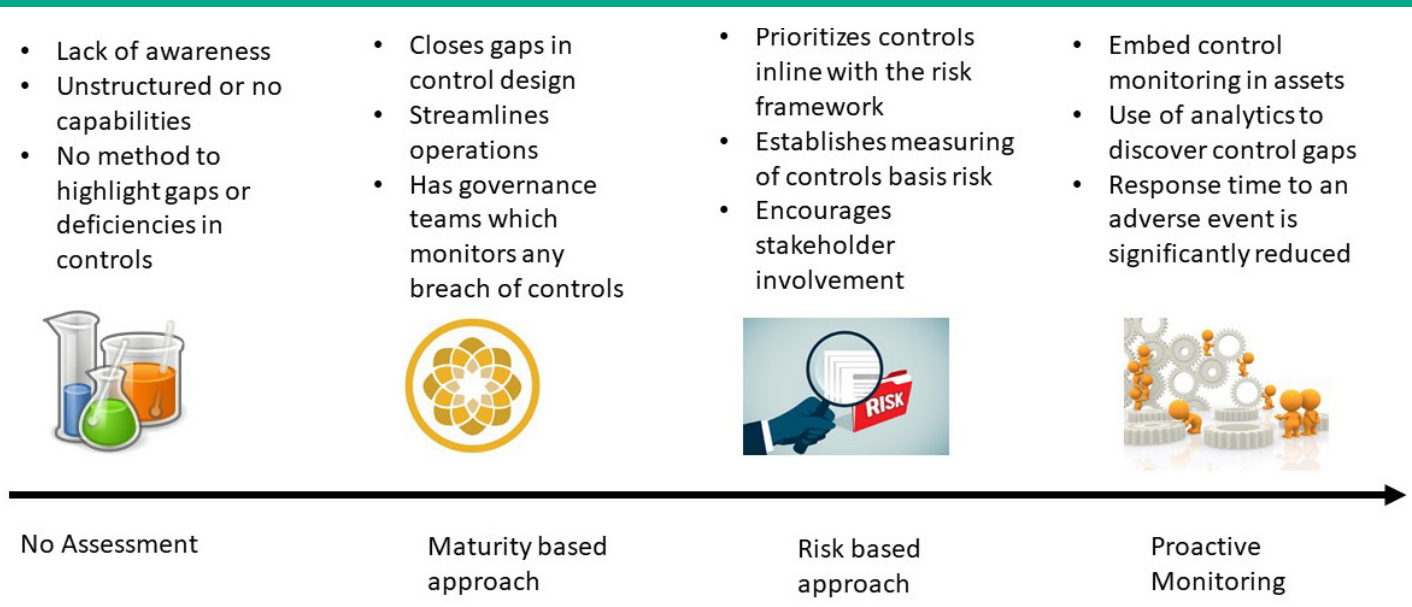
Assessment is not a one-time job. Based on the risk level, the frequency of assessment should be derived. Repeating assessment at a defined frequency helps to keep a check on the controls and their effectiveness. It also helps to identify advanced improvement areas.

Imagining the next

The key focus area of a risk-driven maturity assessment model should be to:

- Support strategic decision making
- Implement targeted improvement initiatives

The outcome of the risk-based assessment is to enable organizations to make quick and sustainable improvements. This is not possible unless the assessment clearly states the recommendations. The risk-driven approach caters to potential risks by providing an appropriate category of controls for corresponding risks. The next step is to embed the controls in services, processes, and products from the point of beginning until execution to achieve complete governance over the control design. To embed these controls, it is advisable to follow a proactive and preventive approach (rather than reactive). This can be achieved by implementing advanced analytics and machine learning for detection. Hence, reducing the risks significantly and improving the response time. The proactive control monitoring would incorporate the stakeholders making the enterprise further agile and resilient.



Evolving timeline of control maturity assessment from no assessment implemented to the future state

About the Author

Divya L.N. Dixit
Principal Business Consulting, Infosys Consulting

Divya has experience in Control Maturity Assessment, Information Security, Risk Management, and Audit Management.

For more information, contact askus@infosys.com

Infosys®
Navigate your next