WHITEPAPER

An Enterprise Perspective on Internal Controls

A guide to mature your internal control program

Business is dynamic and organizations need an agile and mature approach to manage internal controls. Many organizations struggle to monitor and manage internal controls effectively in a distributed and dynamic environment. Too often, internal control management is an occasional exercise to support financial reporting requirements that lacks complete visibility into the organization's processes and systems in context of achieving objectives and mitigating risks.

Immature Siloed and Manual Approaches Compound the Problem

Approaching internal control management as a periodic regulatory reporting exercise is a serious inhibiter to corporate integrity, performance, and risk management. This challenge is even greater when internal control management is not an ongoing and monitored process in the organization that is connected to and enables all aspects of governance, risk management and compliance (GRC).

This problem is compounded when internal control management is siloed within departments and functions encumbered by documents, spreadsheets, and emails. Manual processes are not well suited to understand the complexity and role of internal controls to reliably achieve objectives. An internal control management strategy that is siloed and myopic makes enterprise and operational risk management a challenge.

When an organization approaches internal controls in scattered silos across the business and its operations, there is little chance to be informed and have real insight into emerging risks and the controls that govern their management and mitigation.

SAI360
RISK FROM EVERY ANGLE

Controlling the Dynamic, Distributed, & Disrupted Organization

Today it is critical that GRC roles are all working off the same data and that control data is clean, reliable, and timely. They should also be aligned to an enterprise view of performance, objectives, and risks of the organization. Internal control management is essential to all three elements of G-R-C.

- **Governance.** An organization without controls has no structure to provide consistent behavior and performance.
- **Risk Management.** Controls address risk and are an essential part of risk treatment programs. Enterprise and operational risk management programs can only work if there is a corresponding enterprise internal control management program.
- **Compliance.** Internal controls in the modern organization are more than Sarbanes-Oxley Compliance. Internal controls are put in place to ensure the operational integrity of the organization to meet these obligations.

As organizations improve their approach to enterprise and operational risk management, and broader GRC, it is necessary that the organization adopt an enterprise view of internal controls. A mature approach to internal control management results in predictable business behavior, transactions, access, and processes.

Call to Action

Business requires a robust integrated internal control program. It is time for organizations to assess their current state of internal control management maturity and start building toward their desired state of maturity. The goal is an internal control management program that is effective, efficient, and agile where management can continuously assess controls and their impact on objectives, uncertainty/risk, and the integrity of the organization. Technology for internal control management, automation, and continuous monitoring enables organizations to achieve a real-time, integrated view of enterprise risks and controls across business systems, applications, processes, and roles.

An Internal Control Management Maturity Model

Organizations need a strategy and framework to govern internal control management effectively that aligns with your organization and its objectives. A lack of integration of internal control strategy, processes, information, and technology is not sustainable and leads to inevitable failure as well as risk and regulatory exposure.

Organizations are at various stages of maturity to implement an internal control management strategy with a uniform process supported by an integrated information and technology architecture. Organizations are seeking to modernize and mature internal control management to address the vast web of risk and regulatory requirements that span the organization and its processes to ensure the organization is agile and resilient as it strives to achieve objectives.

Mature internal control management is a seamless part of governance and operations. It requires a top-down view of objectives and risk and becomes a part of the operational fabric of business – not an unattached layer of oversight. It also means bottom-up participation, where business functions identify and monitor internal controls in context of business operations and processes. Increasing maturity within your organization's internal control program is essential to operational agility and resiliency. This enables your organization to ensure that it is governed adequately to protect itself from risk exposure and maintain integrity as it pursues its objectives – it is not only about meeting regulatory requirements.

Maturing your approach to internal control management requires knowing where you are today, this is your current state of maturity, and looking towards the future, your desired state of maturity. This is a three-step process to define your roadmap to improve internal control management maturity:

1. **Understand where you are today –** Your organization must have a firm grasp on where you are in your internal control maturity, as well as an understanding of the risks you are exposed to and requirements that need to be addressed. To progress in maturity requires that you know where you are starting from in order to map out your maturity journey.
2. **Know where you want to be –** After you understand your current state, the next step is to define your future state. Where should the internal control management program be in a few years? What does it look like? What are your key objectives and tactics for getting there? How has it changed and supported the business in a way that is more agile, effective, and efficient? The key here is to define what is right for your organization as there is no one-size fits all internal control management program. Following a maturity framework, as in this guide, will help you map out your journey effectively.
3. **Map out the internal control management maturity journey –** Once your organization understands the current state and defines the future state that you are aiming for, the next step is to roadmap the project plan, tasks, milestones, and activities to move the organization from the current state to the desired future state. Three-year plans are the most effective as they give you time to progress and achieve your goals, modifying as you need to.

STAGES OF ICM MATURITY

Initial
Repeatable
Defined
Managed
Optimized

SAI360 has developed this internal control management maturity model to articulate maturity in internal control management processes and provide organizations with a roadmap to support acceleration through their maturity journey.

There are five distinct stages to the internal control's management maturity model, and you will find that your organization is somewhere along this path and may have even passed through multiple stages:

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimized

1. Initial

Organizations at the Initial stage of maturity have siloed and reactive approaches to internal control management that vary between departments. Businesses at this stage fail to map internal controls to risk and is more focused on a periodic evaluation of controls for compliance purposes and to satisfy external auditors and regulators. Few if any resources are allocated to internal control management. The organization addresses controls in a reactive mode — documenting controls and conducting assessments when forced to. There is no structured group or accountability for monitoring of internal controls, and certainly no integration of internal control information and processes in context of corporate objectives.

Here is a checklist of elements that identify if your organization is at the Initial stage:

- **Blind spots:** Businesses at this stage are subject to many blind spots. Understanding of internal controls and risk exposure to objectives is vital and the organization is caught off guard.
- **Reactive:** The organization addresses internal control management in a reactive, firefighting mode e.g., completing assessments when forced to.
- **Lack of ownership or accountability:** No one has been appointed to take control of an internal control management strategy.
- **Lack of process:** There are no defined or consistent processes or methodologies for managing internal controls or the risks that they expose the organization to.
- **Under resourced:** Few resources are allocated to internal control management.
- **Manual:** There is little to no technology deployed for internal control management with a reliance on documents, spreadsheets and email.

Technology at this stage is about manual processes done with documents, spreadsheets, and emails. There is no defined technology architecture for internal control management, and the cost is in inefficiency in time and ineffectiveness in a robust system of record of internal control activities. Reporting takes a lot of employee time.

Getting to the Next Stage

Departments at the Initial stage have siloed approaches to internal control management at the department level. This means no integration or sharing of internal control information and related risk and compliance information, processes, or technology. An organization that sees itself at the Initial state stage should skip the Repeatable stage, and plan to move to the Defined stage. This is done by developing a department level strategy, unified processes, and implement an internal control management solution that can meet the needs of the department and grow with the solution as it continues the journey to higher levels of maturity.

2. Repeatable

The Repeatable stage sees scattered departments with some regular focus on internal control management within respective functions, most often finance/accounting and IT. However, information and processes are highly redundant and lack integration. With siloed approaches to internal control management, the organization is still very document centric, but technology is starting to be used to replace these manual processes. Processes often remain manual and lack standardization, making it hard to measure effectiveness.

Here is a checklist of elements to determine if your organization is at the Repeatable stage:

- **Pockets of good practice are emerging:** Your program may have some pockets of good practice emerging within departments, but they need joining up.
- **Blind spots:** Businesses at this stage are still subject to blind spots, especially across the organization as much internal control information exists in departmental silos.
- **Inefficient:** Functions are working hard to address internal controls in some silos, but without a full picture of internal controls mapped to risk and objectives across the organization there are a lot of duplicated efforts.
- **Disconnected:** Internal control management is still being addressed in a disconnected way. Disconnected across departments, disconnected across processes, and disconnected across systems. Not only is this inefficient, but it also means internal controls can be costly as there is no common view of controls where a control can be defined once and used for multiple purposes.
- **Limited technology:** With little technology support in place often supported by a reliance on spreadsheets and email, processes fail to be consistent. This can slow your progress, with little ability to audit programs and activities.
- **Hard to measure and monitor:** While some data is beginning to emerge, it's in disparate systems and incomplete.

Departments at the Repeatable stage have siloed approaches to internal control management at the department level. This means no integration or sharing of internal control information and related risk and compliance information, processes, or technology.

Technology for internal control management is scattered and inconsistent. There may be scripts and tools being used to assess controls, but the overall program is still being managed in manual processes with documents, spreadsheets and emails.

Getting to the Next Stage

To move from Repeatable to Defined requires the department to reduce manual internal control data integration and improve overall visibility into internal control management and assessment. Organizations should consider defining internal control management process, technology, and information architecture at the department level and implement technology to manage and automate internal control assessments cohesively within the department.

3. Defined

The Defined stage suggests that the organization has some areas of internal control management that are managed well at a department level, but it lacks integration to address controls across departments to support enterprise and operational risk management. The organization does well at specific compliance areas such as Sarbanes-Oxley (SOX) with Internal Controls Over Financial Reporting (ICFR).

Organizations in the Defined stage will have defined processes for internal control management within departments or business functions, but there is no consistency between the departments. Internal control management processes have the beginning of an integrated information architecture supported by technology and ongoing reporting but have a lot of room to grow. Accountability and oversight for certain domains such as internal controls over financial reporting and IT controls are established, others are emerging.

Here is a checklist of elements to determine if your organization is at the Defined stage:

- **Better efficiency, but room for fine tuning:** You are beginning to gain efficiencies at the department level through automation but compiling internal control reports across departments is likely to take time, and data is likely to be incomplete.
- **Semi-automated:** You are beginning to automate some internal control management and monitoring processes, leading to better assessment and enforcement, and other efficiencies in parts of your program.
- **Reporting is getting better:** Better reporting and monitoring at the department and compliance levels, but it is still hard to extract an enterprise-view of internal controls mapped to risks and objectives.
- **Governance and oversight are starting to develop:** There is some senior management engagement, and particular risk domains such as internal controls over financial reporting and information security are benefiting from an enhanced level of control oversight.
- **Better vision and transparency:** Businesses at this stage are beginning to eliminate blind spots, with a more integrated view of risks and controls. However, the organization is still blinded at the enterprise view of risk.

Technology is a key differentiator in being at the Defined stage from the Initial and Repeatable stages. It is at this stage that a department has implemented a solution that can document, manage, assess, and report on controls within the department and its processes. Technology is focused on assessments with workflow and tasks, and automation of reporting. However, the organization has not addressed ongoing continuous monitoring and enforcement of controls.

Getting to the Next Stage

Departments at the Defined maturity stage are in a good place to lead the organization in an internal control management strategy to the Managed stage. They have a strategic approach to internal control management at the department level, supported by mature internal control assessment processes that can be extended to other departments.

4. Managed

In the Managed stage, the organization has a cross department strategy for managing internal controls mapped to risks, but a limited view into controls in context of performance and objectives. Internal control management is aligned across several departments to provide consistent frameworks and processes and supports an enterprise and operational risk management program. The organization addresses internal control management through shared processes and information that achieve greater agility, efficiency and effectiveness. However, not all processes and information are completely integrated, and there is not an integrated view of objectives and performance.

Here is a checklist of elements to determine if your organization is at the Managed stage:

- **Good vision and transparency:** The organization benefits from an integrated view of risk and controls across departmental, regional and enterprise levels. The organization is beginning to consider the implications of performance and objectives in control assessments.
- **Greater efficiency:** Silos have been broken down across the organization. It is likely that the organization has started to address continuous and automated internal control monitoring. Time to conduct internal control assessments is decreasing, and all three lines of defense are operating in a single system.
- **Reporting is robust:** Reports are comprehensive and delivered to management about multiple categories of risks and controls associated with business processes. The organization is beginning to assess controls in context of performance and objectives which can contribute to continuous improvement and ROI/value conversations of controls.
- **Fully auditable:** The program has a system with full audit capabilities, so the organization can understand every action that has been taken in the program and whom it has been done by, when.

At the Managed stage the organization provides a consistent approach to managing internal controls across the organization from a risk and compliance context. This is supported by an established internal control management process, information, and technology architecture. While internal controls are understood in the context of the business, it is still focused more on risk and compliance than performance and objectives.

Technology at the Managed stage of maturity has become enterprise in scope. There is a unified ERM/GRC strategy that is supported by an information and technology architecture that maps controls and risks across the organization. There is consistency across departments and functions in identifying, assessing, and managing controls with technology. The organization has started to implement automation of continuous control monitoring and enforcement, but not fully.

Getting to the Next Stage

To move from the Managed to the Optimized stage requires a greater control automation and enforcement along with providing a top-down view of objectives and performance that drills into controls to support objectives. Organizations can leverage internal control insight to improve planning and strategic decisions. A common governance model for internal controls is used across lines of business, functions, and processes. The organization needs a common internal control assessment methodology and taxonomy. Organizations at this level report process efficiencies – reducing human and financial capital requirements, greater agility to understand and report on controls, and greater ability to report and analyze controls in context of risk and compliance.

5. Optimized

The difference between the Managed and Optimized stages is primarily one of context and automation. At the Optimized stage the organization provides a consistent approach to managing internal controls across the organization from a performance as well as risk and compliance point of view. This is supported by an established internal control management process, information, and technology architecture that not only assesses controls, but automates the ongoing continuous monitoring and enforcement of controls. At the Optimized stage, the organization has performance, strategy, and objectives setting the context for internal control management.

At the Optimized maturity stage, the organization has completely moved to an integrated approach to internal control management across the business that includes an understanding of controls in context of risk and compliance as well as performance and objectives in business processes. Consistent internal control management processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for internal control management and automation with minimal overhead.

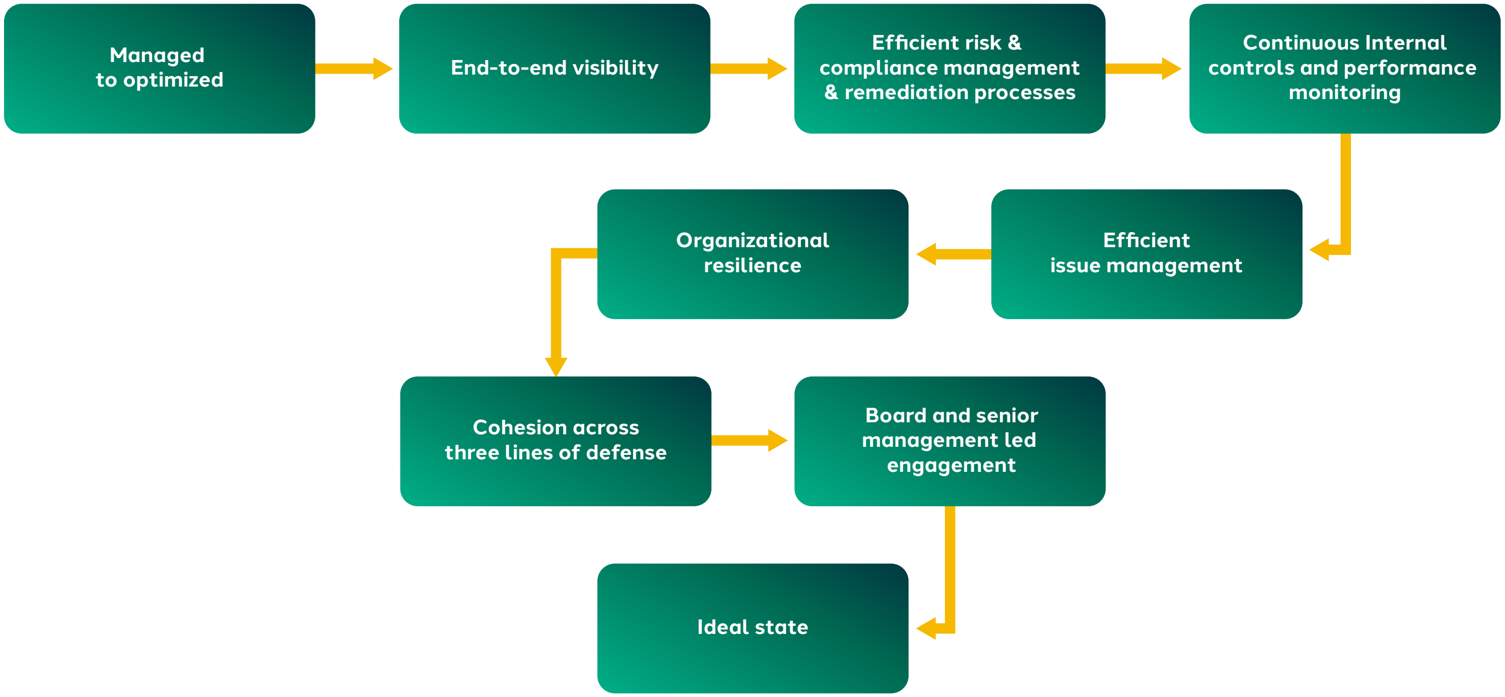
The Optimized maturity stage is where most organizations will find the greatest balance in collaborative internal control governance and alignment. It allows for some department/business function autonomy where needed, but focuses on a common internal control governance model and architecture that the various groups participate in. The Optimized stage increases the ability to connect, understand, analyze, and monitor controls and underlying patterns of performance, risk, and compliance in context of controls. It allows different business functions to be focused on their areas while reporting into a common governance framework and architecture. Different functions participate in internal control management with a focus on coordination and collaboration through a common core architecture that integrates and plays well with other systems.

Here is a checklist of elements to determine if your organization is at the Optimized stage:

- **End-to-end visibility:** Full visibility of governance risk, compliance and performance throughout the organization in context of internal controls.
- **Proactive ability to identify risk, compliance and performance issues and remediate control issues quickly and effectively:** Internal control automation allows for situational awareness to ensure that risk is continuously mitigated within risk appetite of the organization.
- **Continuous monitoring of internal controls and performance:** If defined risk thresholds are met, appropriate internal control actions are automatically triggered. Established data and predictive analytics mean issues can be identified before they become a problem.
- **Issue management rarely needed:** When required, it is resolved quickly and effectively.
- **Organizational resilience:** You understand your critical risks and internal controls help maintain operational agility and resiliency. There are internal control plans and playbooks in place in the event of a ‘crisis event’.
- **Cohesion across three lines of defense:** Lines of business, compliance, risk, audit and senior management are all working in a coordinated way.
- **Board and senior management led engagement:** Senior management champions the program. Periodic meetings with the board and regular governance review meetings ensure senior management is fully engaged and well informed about the effectiveness and strategies internal control governance.

Achieving the Optimized stage requires internal control expectations set as part of the annual strategic planning processes. The organization has measured and monitored controls in the context of business strategy, performance, and objectives. There is shared data and technology about controls, as well as decision support, optimization, and business intelligence. The organization has automated continuous control monitoring and has situational awareness of risk and finance data to drive performance, while mitigating risks and ensuring integrity across the organization.

Approching the optimized state of internal controls


Managed to optimized
End-to-end visibility
Efficient risk & compliance management & remediation processes
Continuous Internal controls and performance monitoring
Efficient issue management
Organizational resilience
Cohesion across three lines of defense
Board and senior management led engagement
Ideal state

Improving Your Internal Control Maturity

Organizations with internal control management processes siloed within departments operate at the Initial, Repeatable, or Defined stages. At these stages internal control management programs manage controls at the departmental level, and lack an integrated view, with no gain in efficiencies from shared processes. In the Initial and Repeatable stage, the organization relies on manual processes encumbered by documents, spreadsheets, and emails. It is only at the Defined stage that the organization begins to leverage technology at a department level to make internal control management more efficient and effective within that department.

The Defined stage is an acceptable maturity level for a department view of internal control that has solid reporting and monitoring of internal controls. An integrated GRC platform that documents, manages, and monitors internal controls is essential to this level of maturity. But it is also necessary to select technology that allows the organization to grow beyond Defined to the Managed and Optimized level as the organization gains an enterprise view of controls mapped to an enterprise view of risks, obligations, and objectives.

In the Managed and Optimized maturity levels, organizations have centralized internal control management oversight to create consistent programs around the world with a common and automated/continuous internal control process, information, and technology architecture. These organizations report process efficiencies reducing human and financial capital requirements, greater agility to understand and report on internal controls in context of risk and objectives/performance, and greater effectiveness through the ability to report and analyze internal control data. The primary difference between the Managed and Optimized stage is the integration of internal controls in the context of performance, objectives, and strategy aligned with the organizations GRC, ERM, and ORM strategies. Differences may be seen in top-down support from executive management, and when various risk and compliance functions align with strategy to collaborate and share information and processe.

Conclusion

A mature internal controls management program is a seamless part of your organization's operations. Internal control management has to be integrated into the culture of the business and this requires both an effort from the top and bottom of the organization to adequately define and guide this culture and participate within it, meaning business functions need to effectively and efficiently monitor internal controls.

In a dynamic business environment where potential, emerging risks lurk around every corner, a mature internal control management program is the bedrock to reliably achieve objectives, address uncertainty, and act with integrity. This framework ensures that all employees and stakeholders involved in business processes and operations management are collaborating with the same key points of data and information, and that everyone involved within the organization understands their specific role, responsibilities and accountabilities. It minimizes the potential consequences of a control failure, risk exposure, or violation of rules, and allows the organization to operate within the expectations of senior management.

Interested in learning more about SAI360's internal control solutions?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE