SAVIYNT

# Three Steps to Application Access Governance Maturity

## Get Clean, Stay Clean, and Optimize

Rapid cloud adoption has introduced new challenges for IT and security teams to implement consistent, effective Governance, Risk, and Compliance (GRC) processes across all cloud and on-premises applications. As the threat landscape changes, the need for tighter security is ever-increasing: cyberattacks and data breaches are on the rise – and these events can do significant damage to your organization. Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley Act (GLBA) were regulations developed in response to financial improprieties. They were intended to force businesses and especially financial institutions to adopt best practices and adequately utilize technology. Violating either of these regulations is costly, and there is a solid track record of enforcement. For example, banks have been fined $243 Billion for non-compliance since 2008.

But implementation is easier said than done. On average, companies use 34 SaaS apps across their enterprise – and as Crown Jewels continue to move from on-premises to the cloud, single and cross-application security and governance become even more critical. Organizations often tackle their full environment by starting with their key financial system, and then including relevant and interactive systems that are in scope for SOX, HIPAA, etc. This continues until they can address the full scope of their environment.  Irrespective of where applications lie in the maturity process, following these steps helps further an application's governance maturity, ensuring continued compliance and standardized monitoring.

This is where governance best practices come in. The goal of any governance program is to clean your environment, maintain that state going forward, and

TABLE OF CONTENTS

and optimize governance and risk management practices. Companies can accomplish this by looking to the Capability Maturity Model for establishing standardized, measured, controlled, repeatable processes that allow for continual process improvement and optimization. We've created a straightforward three-step process to develop a high-functioning risk management program at your organization. We call it: Get Clean, Stay Clean, and Optimize.

## Characteristics of the Maturity levels


## **Get clean:** Establishing a Baseline for the Risk Environment

The first step in creating a standardized and measured process and successfully instituting your risk management approach is to establish a baseline for the risk environment, including single and cross-application Segregation of Duties (SoD).

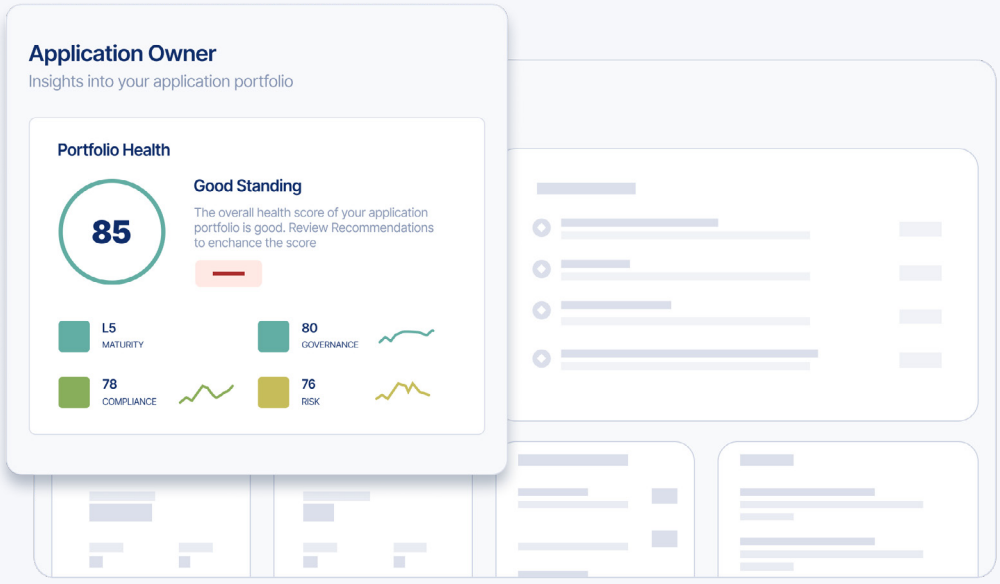
Here's how:

- **ESTABLISH RISK RULESETS**

  Fine-grained segregation of duties (SoD) and sensitive access entitlement rulesets for individual applications – and cross-application checks – ensure that the business has a baseline for its customized risk appetite. Customizing the ranking of risks from Low to Critical ensures that industry and company-specific nuances are considered. The established risk rulesets will be the baseline for driving the risk management and governance program forward.

- **EXECUTE SOD RISK ASSESSMENTS**

  Once the company implements risk rulesets, it requires a baseline of the current risk environment. Executing a detective risk report establishes the current state and drives the future state goals. Risk assessment results can be grouped in order of criticality, by process area, or by various other slice-and-dice metrics to determine the order of the cleanup needed.




**Understanding the health of your current application portfolio is critical to cybersecurity**

- **DOCUMENT MITIGATING CONTROLS**

  When cleaning up a risk, there are three options: remediate (remove) the threat from a user, mitigate the risk for a user, or ignore the risk. The choice each company makes is dependent on its risk appetite and audit requirements. A typical example is that Low ranking risks are reported on but do not require any further action. In contrast, Medium and High risks require mitigation or remediation, and Critical Level risks require remediation and are not allowed to remain assigned to users. Mitigating controls are established processes or reports tied to a user risk when threat remediation is not an option. Mitigating controls should document procedures, control ownership, and approved control risks.

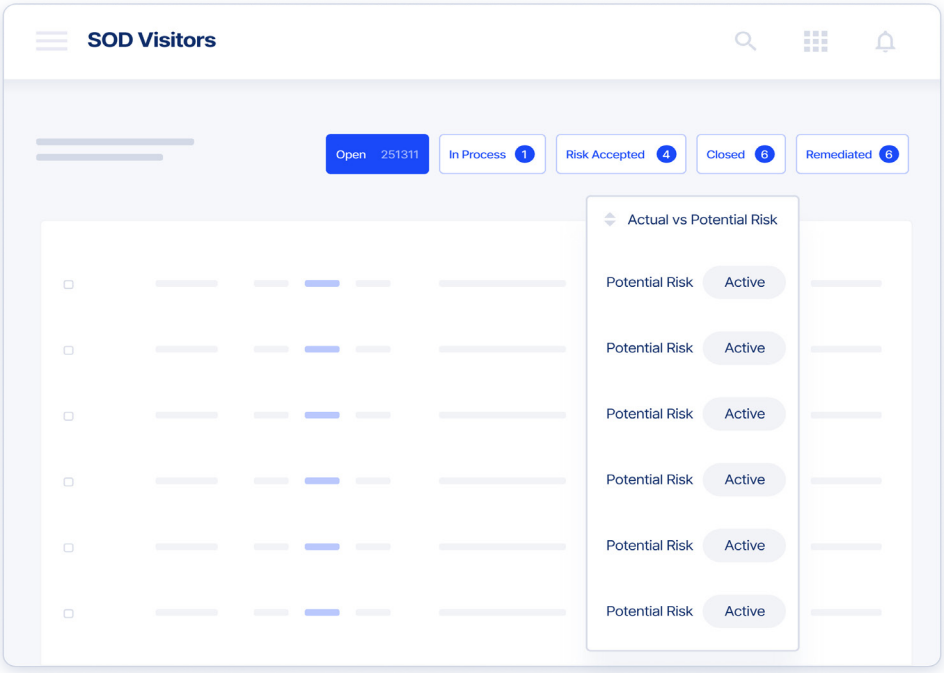
- **ADDRESS RISKS IN SOD REPORTS**

  Once the risk environment has been baselined and approved mitigating controls are documented and mapped to approved risks, it is time to clean the environment. Based on the established risk appetite, each user risk should be flagged for reporting, remediated through the removal of the access causing the risk or mitigated by applying an approved control. The successful completion of this step moves the company into a point in time "clean" environment.

## **Stay Clean:** Instituting Repeatable, Automated Processes with Preventative Controls

Now that the initial risk environment has gone through detective controls and mitigation/remediation, the next step in your journey to a high-functioning governance risk management process is to institute repeatable, automated processes with preventative controls that ensure that your clean environment stays clean. The recommended actions are to:

- **IMPLEMENT ACCESS REQUEST WORKFLOWS**
  Access request workflows ensure that all identity events (joiner, mover, and leaver) are addressed by requiring proper access approvals and preventative risk analysis checks before access changes are completed in the system.
- **ENABLE ACCESS CERTIFICATION**
  Scheduled access certifications keep the environment clean by ensuring no stale access remains for users as job responsibilities change. Access revalidations should be completed in alignment with audit-approved frequency for each application.
- **ENABLE EMERGENCY ACCESS**
  Enforcing a standard of no standing elevated access keeps the environment secure by limiting critical system access and requiring approvals and monitoring for any approved and provisioned temporary emergency access.
- **REMEDIATE RISKS BASED ON ONGOING USAGE MONITORING**
  As users continually use various application functionalities, request access changes, and pass-through access recertifications, their actual usage of different functions should be evaluated to remove any excess (or no longer required) access. Continual usage monitoring ensures that user access needs are met with the least privileged access approach in mind.




**Comprehensive visibility identifies real versus potential risks**

## **Optimize:** Utilizing Built-in Controls, Integrated Risk Simulations, and Role Entitlement/Engineering Management Tools

Reaching the final stage of the Capability Maturity Model can be accomplished by employing built-in controls, integrated risk simulations, and role entitlement/engineering management tools. These allow you to focus on continually improving your environment after establishing a documented, repeatable, and automated risk management process. This enables creating a secure and governed environment that is maintained through visibility.

At this point, existing detected risks have been addressed – and preventative risk detection, automated access provisioning, certifications, and emergency access requests have been implemented. You can now optimize the environment by managing and monitoring environmental controls on an ongoing basis, establishing a complete customer lifecycle end-to-end, and avoiding gaps that may result in an audit and compliance concerns. Here are the steps:

- **UTILIZE ACCESS ANALYTICS**
  Instituting automated persistent controls monitoring, standardized documentation & training on governance processes, and enforcing maintenance of rulesets for functionality usage changes, ensure that the environment maintains a clean user-risk population (i.e., no unmitigated risks exist for users) and meets the end goal of a managed and monitored environment. Out-of-the-box controls from key regulations like SOX, GDPR, HIPAA, etc. are provided and can be customized to establish measurable KPI's.
- **UTILIZE ROLE MINING/ENGINEERING**
  As access utilization changes in applications, role entitlements should be updated accordingly. Part of optimizing a system is continually monitoring usage and functionality changes to reduce excess access and meet the least privileged access goals. When a governance process has achieved a "clean" status, security managers' focus and freed-up time can be shifted to analyze design patterns and access usage for ways to better align entitlements to user needs.
- **MANAGE LICENSES**
  Ongoing license management reviews ensure that licenses are reclassified as user functionalities change. This reclassification maintains a license structure that reflects the actual business usage and avoids cost overages due to incorrect license assignments.

## Lifecycle Steps to Implementing Application Access Risk Management

### Get Clean

- Establish Risk Rulesets
- Execute SoD Risk Assessments
- Document Mitigating Controls
- Address Risks in SoD Reports

### Stay Clean

- Implement Access Request Workflows
- Enable Access Certification
- Enable Emergency Access
- Usage based on-going remediation of risks

### Optimize

- Utilize Access Analytics
- Utilize Role Mining/Enginerering
- Implement License Management

Applying the Capability Maturity Model to your governance and security program allows you to establish standardized, measured, controlled, repeatable processes that enable continuous process improvement and optimization. Once your organization Gets Clean, Stays Clean, and Optimizes, you can govern who gets access and how, secure what access is provided, and maintain complete visibility to access risk and compliance initiatives on an ongoing basis.

**For more information or to schedule a demo, please visit saviynt.com**

SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution. Learn more at **Saviynt.com**

Want to talk to an identity and security expert?

**Schedule a Call Today**