PATECCO
dynamic identity systems.

Since 2009. High Expertise in Identity and Access Management Competence

December 2021

How can Management, Audit and IT Simplify the Identity Governance Process Using Security Verify Governance

WHITEPAPER

- Goals of IGA Project
- Challenges
- Proposed solution
- Risk analysis with SVG Access Risk Control

Table of Contents

How can Management, Audit and IT Simplify the Identity Governance Process Using Security Verify Governance

The need for Governance products has become the norm for large organizations to prevent tampering of identity and access. Organizations are increasingly using risk control like role mining, certification campaigns reporting to control both internal and external threats.

Identity and Access Management (IAM) is a very large area that must balance people-processes and technology. It usually requires a group of IAM solutions that can handle this task holistically. A successful IAM project requires very close cooperation between the IT department and the business units so that the Identity Governance and Administration (IGA) requirements can be reflected in the IT systems according to the operational separation of functions.

O Goals of an Identity Governance and Administration (IGA) Project

- Reduction of administration in IT (saving of work for administration and helpdesk)
- Automation of IGA processes (faster Lifecycle processes, reconciliation, reduction of human errors)
- IT Security risks reduction (least privileged, SoD/SA, restricted access catalog, password policies)
- Supporting legal and regulatory compliance (easy and fast recertification, reporting)
- Reduction of operational costs (audit costs, application licenses, time savings)

O Challenges

To better understand the challenges, we should know what Identity Governance and Administration (IGA) means.

IGA is a set of processes and associated roles and controls that must be implemented by process owners in their respective areas of responsibility.

IGA covers everything that relates to the business, technical, legal and regulatory concerns of an organization.

This means that in addition to the requirements of day-to-day business, the specialized department must also ensure compliance with laws, regulations and compliance such as ISO 27001.

The goal is to answer following questions:

- To know who the person behind the account[1] is.
- To know why the person should have the access.

In these scenarios, a business department manager should be able to understand the IT requirements.

On the other hand, the IT Executive needs to understand the business requirements and make the IT simpler for the end user to ensure secure and productive experience.

The only way for business and IT to achieve this common goal is to work together. The first step in this case is to agree on a common "wording", a list of acronyms and definitions that everyone understands. [1]For example, this must be understood that there is a huge difference between a "User" and an "Account", or that the IT Role "ENPS_GESTSTATI_RILTEC", which is (perhaps) obviously self-explanatory to IT, is meaningless to a CxO, line manager or user.

O People – Processes – Technology

An IGA strategy is not only a technical task, but a complex design that can also impact the organizational structure and requires people to take responsibility. To implement proper segregation of duties (SoD), the organization needs at least one user manager, department manager, risk manager, and application manager with different responsibilities and scopes to avoid a single person having multiple roles and responsibilities that can easily run into SoD violation.

The second step is to mirror business processes back to IT.

After 20 years of IAM/IGA, a number of powerful processes have been defined that can cover almost all IGA use cases and are considered standard, such as joiner-mover-leaver, role creation, role change, access recertification…

When defining a process, it is important to understand the scope of IAM/IGA. For example, "ordering a new computer for an employee" is an HR process, not an IAM process. The good news is that IAM can trigger it. That is, if a computer is not delivered by the vendor, the HR process might still be open to the joiner, but for IAM's point of view, it is already complete!

When selecting a tool, it is important to ensure that the real-world process environment can be mirrored in IT as closely as possible.

O Reduction of Security Risks

- Deleting of orphan accounts
    - The account "might" still have access to exposed resources such as: email, web applications, business premises
    - Malicious external users can use this access as an entry point to the organization
    - Malicious internal users may use this access to bypass personal security controls and "accountability"
    - Standard security policies are unlikely to detect a "correctly" created user

- Enforcement of centralized access rules
    - Access control polices avoid threat correlation (Sensitive Access (SA)
    - Avoid Segregation of Duties (SoD) risks by assigning multiple conflicting roles to a single person
    - Implementing application processes for access permissions
    - Implement processes for "Periodic Recertification of Access Permissions"

- Uniform access rules across system boundaries
    - Management of password policies on all target systems

- Regular review of rules, recertification
    - Regular generation of IGA reports
    - Advanced monitoring through integration with a SIEM system (e.g., QRadar)

O **Proposed Solution**

Modules to cover the use cases with IBM Security Verify Governance (SVG)

Lifecycle

- User Management (create, modify, activate)
- Account Management (Accounts and Entitlements Management)
- Provisioning & Reconciliation
- Access Request Workflow & Password Management (User Portal)
- Reporting

Compliance

- Access Certification
- Risk Management - SoD, SA

Analytics

- Role Mining and Modelling
- Risk Scoring
- Role Lifecycle

O Compliance with Recertification campaigns

For movers, some roles are transferred, and some are assigned as birthrights. These transferred roles must be checked to see if they are associated with a "Visibility Violation" warning or create and SA or SoD risk for the new organizational unit. These campaigns can be recertified at one or more levels.

Certification campaigns in SVG are designed to identify and mitigate entity (user or OU assignment, account, privilege, or risk) risks. Certification campaigns can be customized and extended to meet the required needs, e.g. custom rules (Rules) to detect defined attributes.

If we focus only on user access recertification, there are often requirements for multi-level recertification. This can be done with two parallel campaigns and with predefined rules in the certification campaign record.

One of the new functionalities is that the complexity of certification campaigns is significantly reduced.

The solution delivers user assignment campaigns by default. A distinction as to who should recertify is based on defined hierarchies, applications, or authorizations. What is new is that all these elements are combined in a meaningful way in the configuration of the campaign.

With a user approval option, an administrator can be given the option to close the review with a bulk operation.

There are a few other improvements, such as a progress bar that shows for both the reviewer and supervisors the progress of their campaigns.

It is particularly interesting, in addition to the multi-stage campaign, the option to create a lookup table with predefined multiple choice options for revocation notes, which itself saves valuable campaign review time

O Lifecycle of Roles in SVG Workflows

The module "Process Designer" administers all process steps, workflows, escalation and direct processes.

The process designer covers specific processes, such as passive overview of all applications through application reports or active overview of daily work for a specific administrator role.

Active and passive in this part means that a user can interact with pending requests, approve, or reject them, while passive only provides an overview of the request details. An enhancement in this section is the sorting of tasks, which helps an administrator to find and prioritize his tasks with increasingly strong filtering. Another enhancement is the option to cancel a request from the passive request view.

The second type of single-step processes are escalations. They cover escalation of requests not processed in time or requests with detected conflicts (SoD or SA) predefined in the Access Risk Control (ARC) module.

Authorization assignment for a user is a process that is always asked for. Complex workflows with multi-stage approval processes are developed in the solution. These must also identify and mitigate potential risk critical points (SoD or SA).

Workflow, on the other hand, have received important improvements, especially in risk control. Now an administrator can mitigate a risk directly after SVG has identified and flagged it. This is still escalated for review by the risk management team but can reduce always needed time.

The most common workflow request is to add or revoke user access. This is Out of the Box (OOTB) functionality of a workflow but can be split into two separate workflows depending on the requirement. Requirements can vary in terms of the number of approval steps or administrator roles required to oversee those steps. For example, a workflow may be provided just for assigning user access, which is usually much more complex than that for revoking it.

This process often requires a conflict escalation step that switches processes in SVG from the active workflow to the escalation process and back when that escalation is approved and mitigated. Depending on the configuration, additional approval steps may be required for user managers, application owners, or permission owners. All of this is provided by default and does not require any customization, which is of course possible via the process designer rule engine.

O Analytics – Risk analyses with SVG Access Risk Control

Information coming from different sources poses different risks that need to be handled and brought under control.

The analysis of two types of risk (SoD and SA) is powerful tool of IGI. The risk management team can import their prepared risk data, such as risk tables, which the Access Risk Control (ARC) module uses to analyze authorizations.

The translated data is in an understandable format for business line managers, which is a key advantage of SVG.

The imported process steps (Business Activities (BA)) are mapped in a risk matrix in the solution. They correspond exactly to the risk matrix of risk management. The process steps are assigned to the concrete system authorizations at the lowest level and analyzed in each combination for risks.

Thus, the system must hold risk mitigation information for specific groupings of business activities to indicate automatic risk detection.

After synchronizing all this information for the active configuration set, SVG begins analyzing the defined risks and displays flags for any users or roles that contain conflicting permissions.

These analyses always run in the background and show the current situation for each generated request or created role. In this way, a predefined flag is displayed for each request/role, depending on the severity of the risk that needs to be mitigated.

O Conclusion

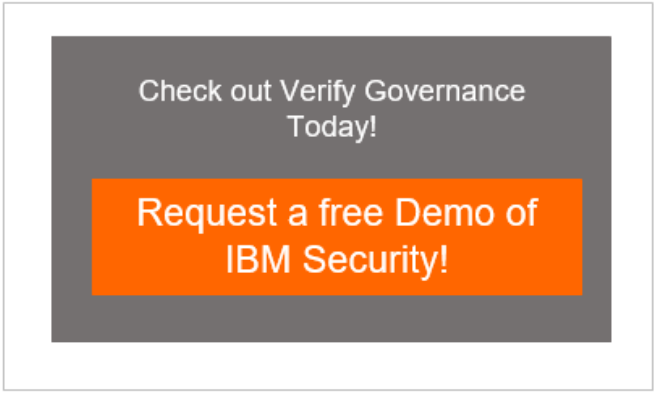
Compliance and corporate governance continue to be key drivers for IGA and IAM projects.

Tracking user access, management approvals, risks, and documentation of who accessed what data and when is an important part of regulatory compliance and can ensure a smoother audit process.

IBM Security Verify Governance (SVG) is a powerful IGA solution that supports regulatory compliance. SVG automates audit reporting and simplifies compliance processes.

Efficiency, security and compliance are important keys to identity and access management. The benefits of a strong IGA solution are clear. The complexity of IGA projects and the cost of implementation can easily be underestimated and derail the organization. A robust IGA solution creates efficiencies in the organization’s operations in the form of automated provisioning and de-provisioning. User productivity is greatly improved while costs are reduced. The burden on IT is reduced and the organization is provided with comprehensive data that helps with regulatory compliance.

To learn more about how IBM Security Verify Governance can benefit your organization with lifecycle management, compliance and analytics, read the following report and request the IBM Security Verify Governance DEMO now via https://www.ibm.com/de-de/products/verify-governance link.



Our IAM experts will be happy to provide you an initial consultation to discuss the factors that need to be considered in order to successfully implement your IAM project.

Call us today to schedule your first free consultation.

Ready to get started?

Talk to an IAM Expert Today!

Get in touch with us:

72 Ringstrasse; 44627 Herne, Germany,

+49 (0) 23 23 987 97 96; info@patecco.com www.patecco.com