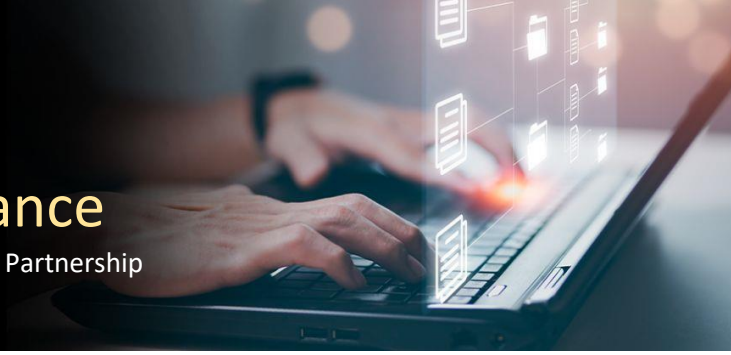
# IBM Verify Identity Governance

Next-Generation Identity Governance and the BBS Strategic Partnership



In today's digital environment—shaped by hybrid work models and multicloud architectures—the traditional network security perimeter has all but disappeared. Identity is no longer simply a control point at the edge of the network; it is the organization's most critical and definitive security boundary. **With AI-powered attacks increasing by 56%**, threat actors are no longer merely "breaking into systems"; they are gaining entry by using valid identities. This shift has transformed identity management from an IT operation into one of the organization's most strategic lines of defense.

- Who has access to which resource, with what privileges, and why?
- Is that access still required?
- Does the access comply with corporate policies and segregation-of-duties rules?
- Is access removed promptly when a user leaves the organization?

Bilgi Birikim Sistemleri (BBS) uses **IBM Verify Identity Governance** to manage digital identities and access rights centrally, automatically, and auditably throughout their lifecycle. By aligning identity processes with corporate policies, the solution strengthens security, reduces manual workloads, makes access risks visible, and streamlines audits.

## IBM Verify Identity Governance (IVIG): An Integrated IGA Platform

IBM has redefined its long-standing identity management heritage with a modern vision, bringing the former **IBM Security Identity Manager (ISIM)** and **Identity Governance (IGI)** capabilities together under one strategic umbrella. At the heart of this transformation is an integrated **Identity Fabric** vision spanning every identity type—including people, machines, and privileged accounts.

- ✓ Identity lifecycle management
- ✓ Automated provisioning and deprovisioning
- ✓ Access request and approval workflows
- ✓ Role and entitlement management
- ✓ Segregation-of-duties controls
- ✓ Access certification
- ✓ Identity analytics and risk visibility
- ✓ Audit trails and reporting

IBM's approach removes the barriers between operational account management and strategic governance. Provisioning capabilities that were previously managed independently are now an integral part of centralized governance within IVIG. This consolidation enables organizations to move from siloed administration to centralized governance and gain end-to-end control through a single platform.

### What Is IBM Verify Identity Governance?

IBM Verify Identity Governance is a comprehensive **Identity Governance and Administration (IGA)** solution that manages user identities and access rights throughout their lifecycle. Identity creation, user-account provisioning to target systems, access-request approval, identification of risky entitlement combinations, and periodic access reviews are all handled within a unified governance approach.

The solution helps provision, audit, and report on user access and activity through lifecycle, compliance, and analytics capabilities. It supports the management of identity processes across on-premises, cloud, and hybrid environments under common policies.

### Automate the Identity Lifecycle

When an employee joins, changes roles or departments, or leaves the organization, numerous account and entitlement actions are required across multiple systems. Manual processes can cause delays, incorrect authorization, and access that is not removed on time.

With IBM Verify Identity Governance:

- Identity data can be obtained from trusted sources such as HR systems.
- New user accounts can be provisioned automatically in target systems.
- Access can be updated when a user changes roles or departments.
- Temporary and time-bound access can be managed.
- Accounts and privileges can be disabled automatically when users leave.
- Orphaned, ownerless, and inactive accounts can be reduced.

As a result, users gain faster access to the resources they need, while unnecessary access remains in systems for less time.

## Orchestrate Access Requests with Workflows

Users or authorized managers can request applications, roles, or entitlements through a self-service access catalog. Requests can be routed for approval to the user's manager, application owner, data owner, information security team, HR, compliance, or other responsible stakeholders.

Approval processes can be configured according to the user's role, the risk level of the requested resource, the organization's approval matrix, and segregation-of-duties policies. Automatically applying approved access to the target system reduces manual IT work and human error.


## Role and Entitlement Management

The right access, for the right user, at the right time

Managing every user entitlement individually is not sustainable, particularly in large and complex environments. IBM Verify Identity Governance helps organizations manage access through business and IT roles.

- Business and technical roles can be created.
- Roles can be associated with applications and access entitlements.
- Baseline access appropriate to each user's job can be assigned.
- Overprivileged users can be identified.
- Unused or conflicting roles can be analyzed.
- Role changes can be governed through approval processes.

A role-based model simplifies access structures while supporting the consistent application of enterprise authorization policies.

## Activity-Based Access Governance

Technical entitlements often have names that are difficult for business teams and auditors to understand. IBM Verify Identity Governance can associate technical access with business activities such as "create purchase requisition," "approve order," "create supplier record," or "execute payment."

With an activity-based approach:

- Technical entitlements are evaluated in the context of business processes.
- Risky access combinations are easier to understand.
- Business units participate more effectively in access decisions.
- Controls become more meaningful for audit and compliance teams.

## Segregation of Duties (SoD) and Access Certification

Identifying SoD risks is especially important in critical ERP systems such as SAP. Allowing one user both to initiate and approve a critical transaction can increase the risk of error, misuse, and fraud. **Segregation of Duties (SoD)** controls help prevent conflicting responsibilities from being assigned to the same user.

With IBM Verify Identity Governance:

- Conflicting roles and entitlements can be defined.
- New requests can be risk-checked before approval.
- Access violations among existing users can be identified.
- Risk-acceptance and compensating-control processes can be applied.
- SoD risks in critical enterprise applications such as SAP can be managed.

## Access Certification and Periodic Review

Access that a user once needed may no longer be necessary. Job changes, temporary projects, and manual grants can lead to privilege accumulation over time.

IBM Verify Identity Governance enables access-certification campaigns based on user, group, role, application, or risk level. Authorized managers can approve access, request its removal, document their decisions, and prioritize high-risk access. Recurring review cycles can be defined for critical applications.


## Identity Analytics and Audit Visibility

By analyzing relationships among identities, accounts, roles, entitlements, and applications, the solution helps expose risks such as:

- Overprivileged users
- Access inconsistent with job responsibilities
- Unused entitlements
- Risky access combinations
- Ownerless and orphaned accounts
- Policy violations
- Unusual user behavior

Recording identity and access activities makes it easier to answer who requested access, who approved it, which policy authorized it, and when it was reviewed.

### A Technology Leap with TCO Benefits

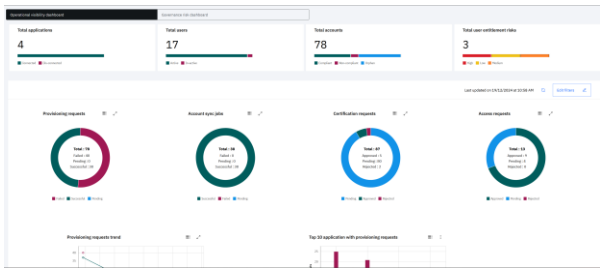
| CAPABİLİTY | TECHNİCAL AND STRATEGİC VALUE |
|---|---|
| **CONTAİNER SUPPORT** | Cloud-native deployment on Red Hat OpenShift and Kubernetes; compatibility with AWS, Azure, and GCP. |
| **INFRASTRUCTURE MODERNİZATİON** | Support for WebSphere Liberty and PostgreSQL. **Removing dependencies on WAS ND and DB2 can significantly reduce total cost of ownership (TCO).** |
| **REST API ECOSYSTEM** | End-to-end automation for DevOps CI/CD processes and seamless integration with third-party systems. |
| **MODERN UI (LOW-CODE)** | A refreshed, modern, and intuitive no-code experience for administrators and end users. |

### Business Value for Your Organization

IBM Verify Identity Governance transforms identity management from a reactive IT operation into a measurable security and governance process.

***Strengthen security***

- Support the principle of least privilege.
- Reduce unnecessary and excessive access.
- Identify risky entitlement combinations early.
- Ensure that access is removed promptly when users leave.
- Reduce insider-threat and privilege-misuse risks.




***Improve operational efficiency***

- Automate joiner, mover, and leaver processes.
- Manage access requests through standardized workflows.
- Reduce the IT workload associated with repetitive account and entitlement tasks.
- Enable users to obtain the access they need faster.
- Limit manual processing and data errors.

***Streamline audit and compliance***

- Create a traceable audit record for access decisions.
- Standardize periodic access reviews.
- Centrally report policy violations and risky access.
- Simplify the preparation of audit evidence.
- Support access-control requirements under the Turkish Personal Data Protection Law (KVKK), ISO 27001, PCI DSS, SOX, and sector-specific regulations.

Using IBM Verify Identity Governance alone does not guarantee regulatory compliance. Processes must be designed in line with the organization's policies, risk approach, and applicable regulations.

### Which Organizations Can Benefit?

- Organizations managing large numbers of users, applications, and entitlements
- Organizations operating on-premises, cloud, and hybrid systems together
- Regulated sectors such as financial services, insurance, telecommunications, healthcare, energy, and government
- Organizations seeking to automate manual access requests and approvals
- Organizations seeking stronger access certification and segregation-of-duties controls
- Organizations planning to modernize an existing ISIM or ISVG environment

## End-to-End IBM Verify Identity Governance Services from BBS

A successful IGA project involves more than product installation. Identity-data quality, role and entitlement model design, application integrations, approval processes, and business-unit participation directly influence project outcomes.

Bilgi Birikim Sistemleri manages IBM Verify Identity Governance projects end to end—from assessment to production, and from training to continuous improvement.

### Assessment and Roadmap

- Assess the current identity and access infrastructure
- Analyze user-lifecycle processes
- Identify authoritative identity sources and target systems
- Evaluate risk, compliance, and audit requirements
- Design role, entitlement, and approval models
- Develop a phased implementation and transformation roadmap

### Architecture Design and Deployment

- Define the solution architecture
- Install and configure the system
- Design high-availability and clustered architectures
- Prepare development, test, and production environments
- Implement security, performance, and capacity settings

### Integration and Application Development

- Integrate HR systems as authoritative identity sources
- Integrate Active Directory, LDAP, and enterprise directories
- Connect enterprise applications, databases, and cloud services
- Develop connectors, adapters, APIs, and custom integrations
- Integrate service-management and workflow systems
- Develop organization-specific processes, screens, and reports

### Governance Model Implementation

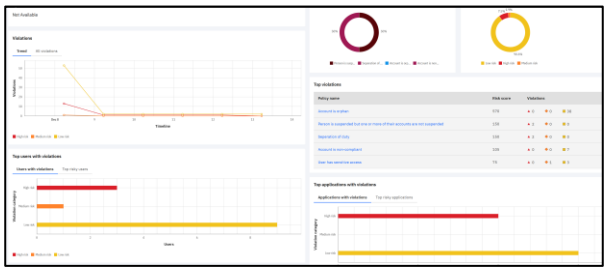
- Design access-request and approval workflows
- Establish the role and entitlement model
- Define SoD rules
- Configure access-certification campaigns
- Implement risk policies and compensating controls
- Prepare audit and compliance reports

### Migration and Modernization

- Assess existing ISIM and ISVG environments
- Prepare the IBM Verify Identity Governance migration plan
- Analyze integrations and customizations
- Migrate identity, role, entitlement, and policy data
- Perform version upgrades and modernization
- Validate and optimize after migration

### Training, Maintenance, and Support

- Provide administrator and end-user training
- Deliver health-check services
- Assess performance and capacity
- Apply version and security updates
- Provide troubleshooting and technical support
- Provide maintenance and consulting services



## Why Bilgi Birikim Sistemleri?

The success of a complex IGA project depends as much on the implementation team's methodology and local experience as it does on the software itself. BBS combines experience in IBM identity and security solutions with deep technical knowledge of legacy ISIM and ISVG environments and strong enterprise-integration capabilities. It designs a practical IGA architecture around each organization's existing investments, security requirements, and business processes. BBS treats every project not merely as an installation, but as a critical part of the organization's digital-transformation roadmap.

### BBS Expertise and Value-Added Services

BBS turns its deep architectural knowledge of IBM solutions into differentiated services in the following areas:

- ✓**Modernization and Secure Migration:** Technical expertise in migrating legacy ISIM or ISVG environments to version 11 while preserving complex customizations and avoiding data loss.
- ✓**IGA Roadmap and Assessment:** Defining the right strategy through health checks and capacity assessments that measure the organization's current maturity level.
- ✓**Custom Integration Development:** Connecting non-standard enterprise applications to the identity ecosystem through SCIM- and REST API-based integrations.
- ✓**Local Regulatory Alignment and Support:** Processes designed with KVKK requirements in mind, together with ongoing post-project optimization support.
- ✓**Post-Go-Live Maintenance and Technical Support**

BBS's technical command of the IBM ecosystem helps organizations maximize the ROI of their technology investments and complete complex migrations with controlled risk.

Looking ahead, this integrated architecture will be strengthened further through **ISPM (Identity Security Posture Management)** and **ITDR (Identity Threat Detection and Response)** integrations. Contact BBS experts to modernize your current infrastructure, simplify complex entitlement structures, and benefit from the TCO advantages of version 11. Let us design a modernization roadmap tailored to your organization.



**Adres:** Yeni Sahra Mah. Fatih Cad. No: 8 Ataşehir / İstanbul P.K 34746
T: +90 (216) 373 98 00
F: +90 (216) 373 99 93