

Sustainable Identity and Access Governance

Table of Contents:	2 Enterprise Access Governance: Some Assembly Required
	2 The Promise of Roles— and the Price
	4 A Compliance Mandate with Operational ROI
	4 Novell Automates End-to-End Access Governance
	6 Governing the Identity and Access Management Lifecycle
	7 End-to-End Business Benefits
	8 Novell Access Governance in Action
	9 A Sustainable Future for IT Access Security



Enterprise Access Governance: Some Assembly Required

Organizations need to bridge the gap between IT and business, eliminate role-related bottlenecks, and create a closed-loop access governance framework that delivers business value far beyond compliance.

Novell delivers the variables required for good access governance: compliance, risk, agility, cost, business assurance and administrative sustainability.

Managing user access to information resources is the beating heart of IT security. Nothing is more basic to securing a network, system, application or database than providing the right access to those with a legitimate business need. Employees should have every resource necessary to efficiently fulfill their responsibilities, and nothing more.

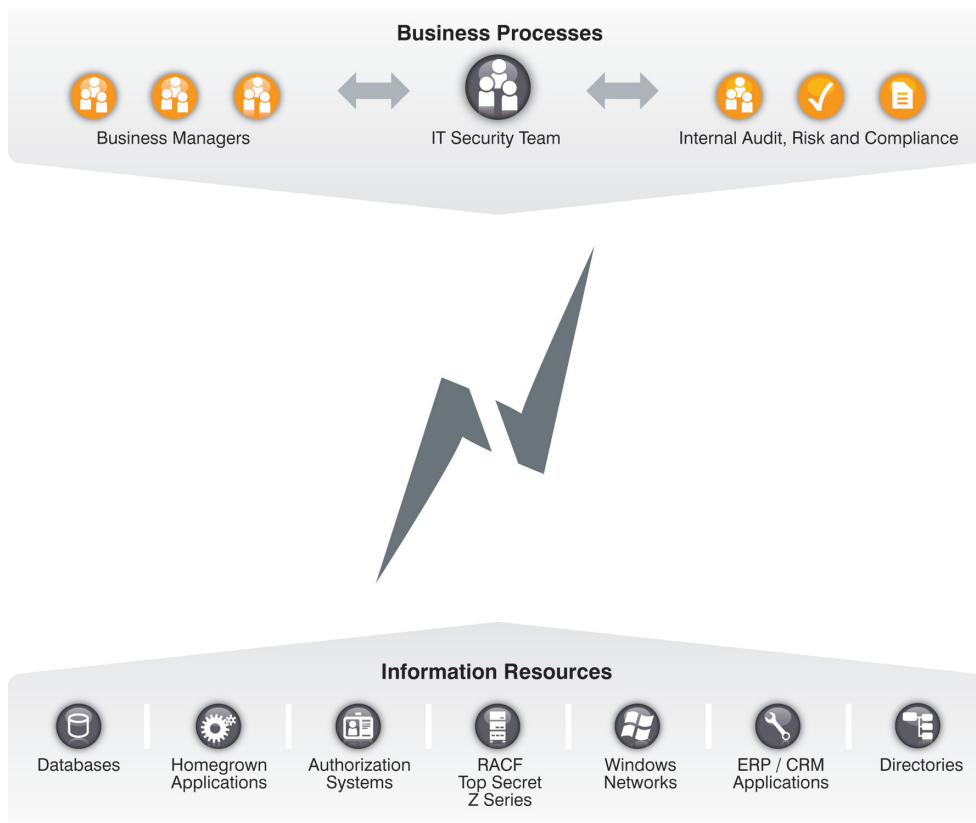
But knowing and delivering exactly the right set of entitlements for every individual has always been difficult, and in today's complex and continuously evolving environments it is quickly becoming impossible—at least with manual tools and processes. Today's enterprise may include tens of thousands of IT systems users and thousands of resources, all of them changing constantly. There is tremendous pressure to provision new users quickly, and security is not the sole measure of success. The entire access management process must comply with an increasing number of internal policies and external regulatory mandates, and process owners must be able to demonstrate continuous compliance. Keeping an organization secure and compliant has become labor intensive to the point that it can seriously compromise operational efficiency, cost management and competitive agility.

The Promise of Roles— and the Price

The most appealing solution is a combination of abstraction and automation: using defined roles to standardize the resource requirements of typical job functions and the individuals who perform them. A combination of events, rules and policy-based workflows can then be used to automate provisioning, validation and compliance processes. Indeed, leading user provisioning and access enforcement solutions—led by Novell® Compliance Management Platform—already support roles, and automated tools are available, whether or not they have been deployed.

But while IT managers may be anxious to use roles to automate access provisioning, they don't have the realistic ability to define those roles on behalf of business users or determine the appropriate resource allocations. They simply don't understand the business requirements or regulatory restrictions well enough to do so. The responsibility for managing roles and access rights must be delegated to the business unit managers who are responsible for the users. Unfortunately, these managers are often poorly prepared and inadequately equipped for that responsibility. They are unfamiliar with the IT environment and use an entirely different language to describe roles and requirements. They have few standards for guidance and only simple manual tools to support their efforts. In fact, spreadsheets are still widely used for access review and certification.

Building a Bridge to Trusted Access



Unified Governance Allows Trust

By combining access certification, role management, provisioning and security in a single solution stack with rule- and policy-based automation end to end, Novell Access Governance Suite supports a number of technical capabilities previously unavailable in most environments.

1 Echelon One (www.echelonone.net)
 2 2007 Global Security Survey, Deloitte

Figure 1. Without Novell solutions, business managers do not have the IT insight needed to manage roles and access.

The result is a slow, labor-intensive role management process that is frequently an operational bottleneck. Security research firm Echelon One reports that manually certifying access rights imposes a 30–40 hour average annual workload on each reviewing manager and application owner, and the burden can be significantly higher in heavily regulated industries that operate under multiple, overlapping mandates.¹

The labor intensity of manual role management translates directly into high operating costs. An organization with 20,000 users might have 500 reviewers. If each one spends 20 additional hours each year manually reviewing, changing and certifying access rights, that's 10,000 hours of lost management productivity. At US\$90 per hour per manager,

it represents \$900,000 of labor expense that could have been more productively invested.

But perhaps most importantly, while manual role and access management processes may fulfill the letter of compliance requirements, they can still expose the organization to significantly heightened operational risk. The Deloitte 2007 Global Security Survey found that 45 percent of respondents had experienced audit findings involving excessive employee access rights, and 35 percent had discovered segregation of duties violations.² CSOs are haunted by incidents like Société Générale's \$7.2 billion loss, caused by a junior trader who was making prohibited transactions using inappropriate system rights that were never revoked from an earlier posting. Even innocent, inadvertent errors

Novell is introducing the Novell Access Governance Suite, a tightly integrated solution set that streamlines and automates access certification, role lifecycle management and risk management.

by users with inappropriate access can be extremely costly.

In fact, the tools and processes many organizations use to manage business roles and entitlement allocations and to demonstrate compliance often become the problem—constituting significant threats to security, operating efficiency, cost control, competitive agility and profitability.

A Compliance Mandate with Operational ROI

Fortunately the solution is clear and the potential payoff is large. Organizations need the ability to extend their IT access management stacks with automated tools that simplify role management and access certification by the responsible business managers. Such an approach will bridge the gap between IT and business, eliminate role-related bottlenecks, and create a closed-loop access governance framework that delivers business value far beyond reliable compliance. Essential components of an integrated solution should include:

For the business side of the organization:

- *Role lifecycle management, including role definition and access allocation, change management and continuous risk management*
- *Access certification and compliance, including automated access discovery, review and certification; compliance analysis; exception response; and remediation*

For IT access management operations:

- *Automated role-based provisioning and access management*
- *Real-time security monitoring, access remediation and reporting*

Where such solutions are deployed, the benefits will inevitably include stronger security, more reliable risk management, vastly improved administrative efficiency, increased operating agility and lower overall costs.

Novell Automates End-to-End Access Governance

To deliver exactly these benefits, Novell is introducing the Novell Access Governance Suite, a tightly integrated solution set that streamlines and automates access certification, role lifecycle management and risk management. These applications are tightly integrated both with each other, and with the core components of Novell Compliance Management Platform. The extended Suite, which consists of Novell Compliance Certification Manager and Novell Roles Lifecycle Manager, lets organizations of any size mitigate access-related business risks, reduce costs and complexity, relieve management workloads and ensure sustainable compliance.

Novell Compliance Certification Manager

makes access governance sustainable by fully automating entitlement monitoring, reporting, certification and remediation. It provides an end-to-end certification process that begins with comprehensive discovery and collection of identity and authorization information from systems and applications throughout the enterprise. It also creates actionable reviews and presents them in easy-to-understand business context tailored for business managers. Business rules enable exception-based entitlement monitoring, and integrated workflows route and track all changes for audit documentation and

compliance reporting. Dashboards and metrics provide fast access to certification and escalation status for both business and security managers. An extensive set of built-in reports combined with ad hoc reporting capabilities deliver detailed and summary analyses of users, applications, entitlements, certifications and compliance status.

Novell Roles Lifecycle Manager provides a holistic approach to defining, creating and managing roles throughout the organization, addressing the distinct requirements of business users, IT security and compliance teams. It shares the discovery and aggregation functionality of Novell Compliance Certification Manager, providing an enterprise-wide view of roles and entitlements. Sophisticated role modeling driven by detailed metrics helps business managers evaluate established roles, define new ones, and accurately allocate necessary entitlements. Change management

workflows support collaboration and provide auditable tracking of all actions. Extensive reporting and analytics monitor the effectiveness of roles and entitlements. An automated certification process makes role owners or designated business managers accountable for reviewing and updating role contents and membership.

The business workflows and role lifecycles managed through the Novell Access Governance Suite integrate with the rich functionality of the Novell Compliance Management Platform. Business roles are provisioned through automated policies to the IT layer. The Novell Compliance Management Platform validates that resources are accessed according to business processes, and then passes this information to Novell Access Governance Suite, ensuring end-to-end access governance.

A Closed-loop Process for Access Governance

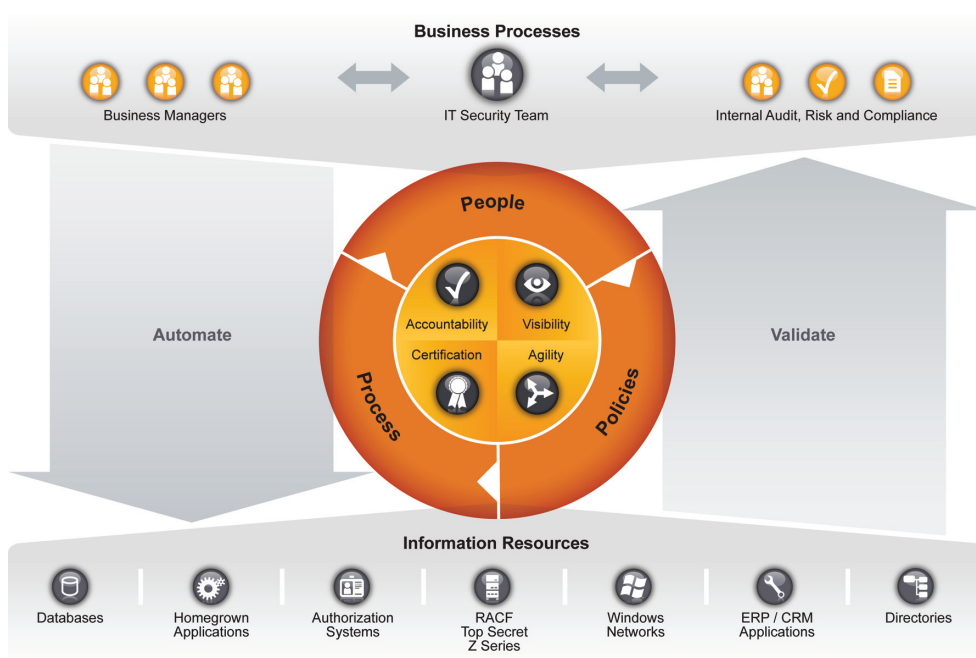


Figure 2. Novell Access Governance Suite unites people, processes and policies to ensure end-to-end access governance.

End-to-End Integration and Automation Enhance Management Capabilities

By combining access certification, role management, provisioning and security in a single solution stack with rule- and policy-based automation end to end, Novell Access Governance Suite supports a number of technical capabilities previously unavailable in most environments, including:

- **Visibility.** *Novell Access Governance Suite securely collects, aggregates and normalizes user access information—identities, user accounts, entitlements and roles—from across all connected systems and resources, providing a composite view of users and their access across the entire enterprise.*
- **User-friendly business context.** *Access information is presented in a business-friendly context, simplifying management and expediting provisioning by making it easier for business reviewers to understand roles and entitlements.*
- **Collaboration.** *Support for collaboration throughout the role management lifecycle makes it easier to engage business managers in role design and allow them to accept ownership.*
- **Process automation.** *All major access management and compliance processes can be fully automated, including access review, certification and reporting, change management and remediation.*
- **Accountability.** *Accountability for governing user access can be driven into the business by providing user, application, reviewer or enterprise-wide visibility of attestation and certification status.*
- **Risk assessments.** *Organizations now have additional tools that help responsible parties understand, monitor, manage and mitigate the business and compliance risks associated with providing users access to information resources, while being able to enforce their business policies in a consistent fashion.*

Governing the Identity and Access Management Lifecycle

The Novell Access Governance Suite—along with established Novell identity and access management products—creates a closed-loop process that automates every aspect of the identity and access management lifecycle. The integration and interaction of these solution components can be seen in each phase of the lifecycle.

Access Certification

Access certification is the process of reviewing and certifying user access rights. This process is required whenever a new application is brought into the environment. Novell Compliance Certification Manager collects existing rights information, presents it for review by the appropriate business approvers, and records all change and approval decisions. Novell Roles Lifecycle Manager supports this process with role modeling analytics that evaluate access allocation patterns for risk and compliance implications.

Role Modeling

Role modeling is the process of defining a roles model based on the certified user access rights, testing and assessing it, and collaborating with others to ensure that the changes are approved and implemented. Novell Roles Lifecycle Manager provides an automated process for role certification and ensures that roles are maintained properly and that appropriate parties are accountable for reviewing role contents and membership.

Role-based Provisioning

Role-based provisioning takes the role and access outputs from the role modeling and certification process and integrates them with user identity information to automate access provisioning to all enterprise resources. Novell Compliance Management Platform ensures that any change in a user's role or status is immediately reflected in access privileges,

enabling first-day productivity and instant de-provisioning on termination.

Access Validation

Access validation is the continuous, real-time monitoring of access utilization. It tracks and analyzes patterns of use and continuously improves access management practice and discipline. Novell Compliance Management Platform provides real-time, event-based inspection to reveal which entitlements are actually being used, and to enable continuous refinement in roles definition and least-privilege access allocation.

Policy and Controls Automation

Policy and controls automation closes the access management loop with real-time, rules-based inspection of access utilization to identify violations and policy exceptions and automatically initiate immediate remediation. The event-based monitoring capabilities of Novell Compliance Management Platform provide direct feedback and notifications and maintain an auditable record of all incident response actions.

End-to-End Business Benefits

Automating the access governance process and integrating it with access provisioning, enforcement and remediation provides significant business benefits that extend well beyond the IT organization and its certification partners in the business organization. The Novell Access Governance Suite allows organizations to:

- **Extend and enforce business policy across all systems and resources.** *Novell Access Governance Suite links business and compliance-access policies into the underlying infrastructure. Organizations can now enforce their access policies consistently across the entire enterprise (applications, data, hosts, systems and network infrastructure) through a centralized approach that leverages existing security*

infrastructure investments such as user provisioning, directories and security information event management.

- **Reduce complexity and cost.** *Eliminate the fragmented, manual approaches that many IT security teams use to manage access entitlements and demonstrate compliance. This offering provides a new automated approach for managing access that reduces complexity and the many costs associated with demonstrating compliance.*
- **Enable dynamic change management.** *By enabling dynamic change management, IT security teams can respond more proactively to access requests. It also expedites access delivery while avoiding potential compliance violations through a closed-loop remediation process.*
- **Drive accountability.** *Provide IT security teams and their business partners with collaborative tools for role management and access certification, risk management, auditing and compliance reporting. This ensures that all constituents participate in access governance through role lifecycle management and automated access certification, driving accountability into the lines of business where it belongs.*
- **Mitigate risk.** *Novell Access Governance Suite helps organizations understand, monitor, manage and mitigate the business and compliance risks associated with granting users access to information resources. And it does all of this while consistently enforcing business policies.*
- **Ensure sustainable compliance.** *Novell Access Governance Suite provides an auditable system of record for access policy management. This includes automation for access requests, enforcement, access-rights remediation, validation and compliance certification. The entire process is streamlined and simplified so that effective access governance can become part of daily operating procedure, and sustainable compliance can be achieved.*

Novell Compliance Certification Manager works in conjunction with Novell Compliance Management Platform to discover user access rights wherever they reside, and then automate the review, certification and attestation processes.

Novell Access Governance in Action

The broad benefits of an integrated access governance solution can be clearly seen in three use cases that are nearly universal in their applicability to access management and compliance operations.

Compliance Automation

In companies that fall under one or more of the large government or trade association regulatory regimes—such as SOX, GLBA, PCI, EU DPD and HIPAA, among others—the IT security organization is typically forced to dedicate significant human, technical and financial resources to reviewing, certifying and continuously re-certifying user access. The process is often complex and resource-intensive because access data have to be manually extracted, aggregated and normalized from every application, directory, database, file, file share, database and firewall. Often, too, the security team has no automated management system for presenting the consolidated information to business reviewers for certification, for managing change requests, or for recording auditable evidence of compliance.

Within the Novell Access Governance Solution, Novell Compliance Certification Manager works in conjunction with Novell Compliance Management Platform to discover user access rights wherever they reside, and then automate the review, certification and

attestation processes. The result is a vast reduction in the complexity, cost and burden associated with compliance.

Change Management

Another area where IT security organizations struggle is in provisioning new user access and access change requests. In trying to respond promptly or meet service level agreements, the IT organization is likely to fulfill a request without evaluating it for potential business or compliance risk. In most organizations, an entitlement change request is a manual process that is fulfilled by the owner of the appropriate application or information resource. These individuals typically have no visibility into a user's other access rights, and no way to evaluate the potential risks or conflicts that might arise from the requested entitlement change. There may also be no automated validation process to confirm the completed change, leading to entitlement drag that can easily give rise to compliance violations or business risks.

Access provisioning and changes are better managed through a continuous role lifecycle management approach that speeds up access delivery while enforcing least-privileged access through entitlement utilization monitoring and ensuring sustainable compliance. Novell Roles Lifecycle Manager works in conjunction with Novell Identity Manager to discover, design, engineer and maintain effective business roles—all while avoiding role proliferation and continuously managing access-related risk.

Access Risk Mitigation

To date, IT security teams have typically been reactive in their approach to risk management and mitigation. As the speed of business increases, this approach doesn't scale. Organizations need a proactive approach based on an understanding of where access-

related business and compliance risks can occur. This approach should also provide embedded support for correct user access decisions and the provisioning and monitoring facilities to implement those decisions. With such a system in place, IT security teams can classify information resources for risk sensitivity and then monitor, manage and mitigate risks against those resources.

Novell Access Governance Suite works with Novell Compliance Management Platform to orchestrate access governance. Together they provide least-privileged rights enforcement, dynamic access violation management, risk analytics and reporting, and automated closed-loop remediation.

A Sustainable Future for IT Access Security

When deployed with industry-standard-setting identity management, roles-based

provisioning and real-time security solutions from Novell, the Novell Access Governance solution links role definition and management with access provisioning, utilization monitoring, remediation and reporting. This approach not only helps organizations become secure and compliant, but it also allows them to become stronger, faster, leaner and more successful. It gives IT security organizations a proven, scalable, and fully automated solution for managing resource access and compliance that will be reliably sustainable under any level of growth and change, either in the organization itself or in the external regulatory environment.

For more information about the Novell Access Governance Suite, please visit the product Web site at: www.novell.com/products/accessgovernancesuite

When deployed with industry-standard-setting identity management, roles-based provisioning and real-time security solutions from Novell, the Novell Access Governance solution links role definition and management with access provisioning, utilization monitoring, remediation and reporting. This approach not only helps organizations become secure and compliant, but it also allows them to become stronger, faster, leaner and more successful.

www.novell.com



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA