Advanced Attestation and Recertification for Today's Organizations

Written by Matthias Bauer, managing director, Dell Software

Abstract

The ever-increasing demand for transparency is causing IT departments to intensify the monitoring of IT permissions. Many organizations, including the heavily regulated banks and insurance companies, are establishing attestation and recertification procedures in order to achieve and demonstrate compliance with industry and governmental regulations such as Sarbanes Oxley, HIPAA, FERC and Basel III.

This paper explains the concepts of attestation and recertification and then details the levels of sophistication organizations can achieve in their traditional recertification processes. Last, it explains how to implement a modern, role-based attestation and recertification architecture.

Attestation versus recertification

Although the terms "attestation" and "recertification" are often treated as synonyms, there are distinctions that are important to identity management and user provisioning.

Attestation

Attestation is confirming that one or more "facts" are truly correct. Examples of attestation include:

- Assigning access permissions (such as AD group memberships, SAP roles and composite roles) to individuals
- Assigning technical roles or access permissions to certain roles or groups, such as assigning ACLs to an AD group or assigning transactions and permission codes to an SAP role
- Assigning system roles to defined business roles
- Assigning employees to business roles

In addition, the attestation process may go deeper into the identity management and user provisioning processes. Examples include:

- Confirming the validity of a compliance rule (such as segregation of duties or an intolerance rule)
- Confirming an approval workflow's validity for specified IT resources
- Confirming that an employee is part of an organizational structure

> Recertification is the ongoing process of revalidating permissions, privileges and entitlements granted to users.

Recertification

Recertification, on the other hand, is the ongoing process of revalidating permissions, privileges and entitlements granted to users. Recertification ensures that users have only the proper authorizations to IT systems and the information in those systems.

Recertification has a high priority in governance, risk and compliance projects. This is particularly true for banks and insurance companies, which are subject to regulations such as such as Sarbanes Oxley, HIPAA, FERC and Basel III, which require proof that the procedures and controls that are in place ensure proper attestation and recertification. Many of those procedures are manual, with staff keying in detailed access privileges for each individual and for all types of systems.

Levels of sophistication for recertification

Organizations tend to fall into one of five levels of sophistication when it comes to recertification, as described briefly in Table 1 and explained in further detail below.

Level 1: No recertification, no regular account reporting

Level 1 has no recertification and no regular account reporting.

Level 2: Recertification as a recurring, manual project

For organizations at Level 2, recertification is a recurring, manual project. A typical example would be an organization that annually creates a report listing people and their permissions for all the various systems, and has department managers review the permissions for their staff, confirming or correcting them.

This approach provides a minimal level of transparency and documentation. However, it has several disadvantages:

- Time and cost — A considerable amount of manual effort is often required to create the reports. It is not uncommon for organizations to export files from individual IT systems, consolidate them manually into Excel tables and have managers review long printouts. Moreover, implementing any changes to the permissions structure identified by the recertification process

Level	Description	Limitations
Level 1: No recertification, no regular account reporting	No recertification, no reporting	No transparency or documentation
Level 2: Recertification as a recurring, manual project	The organization produces an annual report listing people and their permissions for all the various systems. Managers review the permissions for their staff members and confirm or correct them.	Minimal transparency and documentation
Level 3: Recertification of single permissions through automated processes and request and approval workflows	Recertification processes are automated and continuous, with well-documented request and approval workflows	Minimal transparency and significant effort to process individual permission request
Level 4: Continuous recertification on multiple levels using business roles	Using descriptive roles for assigning permissions significantly improves the efficiency and effectiveness of recertification.	No risk management perspectives
Level 5: Recertification using risk management principles	The organization can analyze recertification information from different risk perspectives.	None

Table 1. Levels of sophistication for recertification

typically requires significant additional manual work.

- Poor transparency that can result in over-provisioning — Often the permissions in the report are described in technical terms that are difficult for line-of-business managers to fully understand. Therefore, they may be tempted to simply confirm all the permissions, which increases the risk of users having more permissions than they need to do their jobs.
- Risk of incomplete review — Recertification takes place based on a snapshot of the permissions, which does not necessarily include all permissions assigned since the last recertification. For example, a critical combination of permissions that a staff person held temporarily since the last recertification will not be included in the snapshot and therefore will never be reviewed.

Level 3: Recertification of single permissions through automated processes and request and approval workflows

Organizations can achieve tighter control over the correctness of permission assignments by adopting continuous recertification processes. The initial permissions assigned for these processes are validated through well-documented request-and-approval workflows, and users retain appropriate permissions through recertification.

Continuous recertification is best achieved by implementing an automated identity management system that includes a workflow component. This allows recertification to be processed using the same workflow system as the one assigning permissions, and the automation reduces manual effort. It also avoids the risk of incomplete review present in Level 2, since every set of assigned permissions is determined via a defined and documented process.

However, like Level 2, Level 3 lacks transparency. The names of permissions and entitlements tend to be cryptic — understandable to technical staff but not to the manager who needs to recertify or reject them. Additionally, this approach is not user-friendly, due to the large numbers of single permissions to be managed.

Level 4: Continuous recertification on multiple levels using business roles

Using descriptive roles to assign permissions, rather than assigning permissions individually, offers multiple benefits. The first is transparency: when arcane and technically-oriented IT entitlements are replaced with descriptive roles, responsibility for granting permissions can be moved from IT staff to the business managers who better understand who needs access to what. This in turn reduces the risk of inappropriate permission assignments.

Using descriptive roles to assign permissions, rather than assigning permissions individually, offers multiple benefits.

Moreover, business roles streamline the process of changing a user's permission when technical or organizational changes occur. For example, suppose an employee changes positions within the company, moving from Finance to Marketing. Updating his role assignment will automatically revoke his permissions to access sensitive financial data he should no longer see, while ensuring he can access all the marketing documents he now needs in his new position.

Using roles also helps organizations deal with the challenge of mass attestations, which can arise, for example, due to a comprehensive reorganization or the need for recertification of a large stock of permissions. Instead of blindly hitting the common "Accept all" button, the organization can use a multi-stage attestation process that recertifies users based on their roles in the organization: the department manager attests to only the affiliation of employees to specific roles (such as "Purchasing Manager") without having to know each of the specific permissions associated with each role.

Finally, if desired, the definition of business roles can itself be part of the recertification workflow, enhancing security.

Level 5: Recertification using risk management principles

Risk management practices are quickly becoming the next extension of attestation and recertification processes. Instead of looking at all users, all access privileges or all data, organizations are concentrating on where risk is highest by asking questions like:

- Which systems house the most critical data?
- Who has access to those systems?
- What kind of authority do they have to change things on those systems?
- Is a user's access a violation of separation of duties (Sod)? For example, does a user have both the power to set up a vendor and pay a vendor?

Level 5 recertification systems enable organizations to answer those questions, adding an element of intelligence to the recertification process.

Implementing attestation and recertification

Dell One Identity Manager

How can you implement a modern attestation and recertification architecture that uses business roles to control permission assignments?

With Dell One Identity Manager. Identity Manager is an identity management and user provisioning solution that is designed to manage the complete lifecycle of identities, not just the recertification tasks. Identity Manager includes an entire set of processes and technologies for maintaining and updating digital identities. Its identity lifecycle management capabilities include identity synchronization, provisioning, de-provisioning, and the ongoing management of user attributes, credentials and entitlements.

Attestation and recertification architecture

Identity Manager's architecture consists of two major components:

- **The attestation object**, which is, in principle, an interactive report for attestors (see Figure 1). The design of this report is critical: notice that it displays all the relevant information needed by the attester while still providing a clear overview of the process.
- **The attestation policy**, which specifies who should perform attestations for each object, including how and under which conditions.

This architecture not only meets the highest levels of sophistication and provides the security required by many regulations throughout the world, but also enables the management of data more complex than permissions, such as:

- Objects such as processes, personal statuses, request and approval workflows, business roles, ITShop articles, web front-end versions and compliance rules
- Triggers, which in addition to normal scheduling triggers can include user additions, changes, moves, deletions or disabling

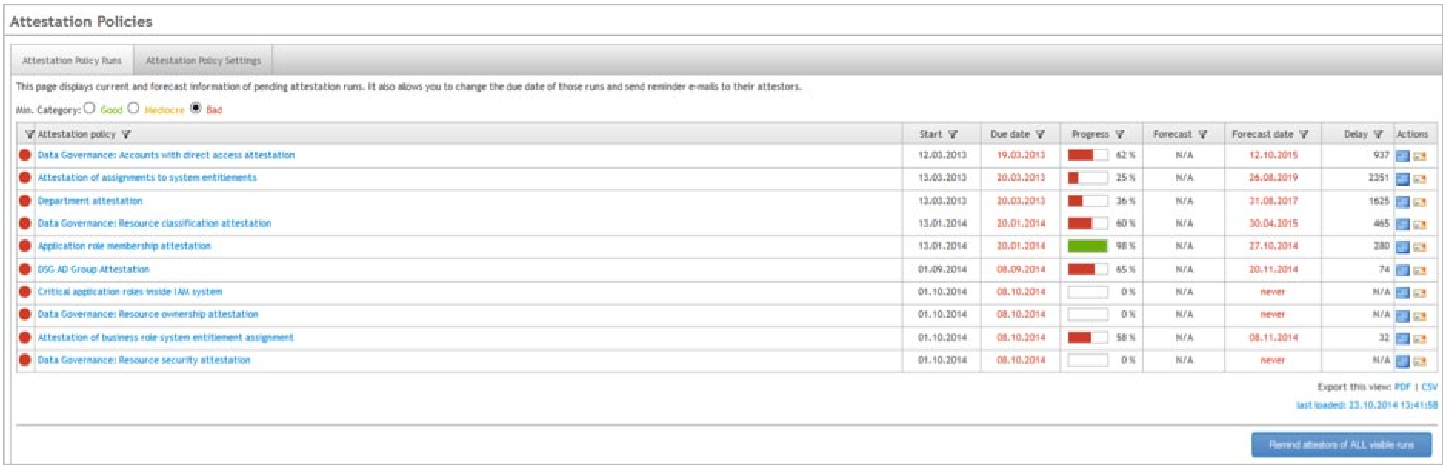
Attestation and recertification dashboards

Dashboards are useful monitoring tools, helping organizations achieve effective status control, regardless of whether attestation and recertification are implemented as a continuing process or as single projects.

A typical dashboard displays tables listing the state of multiple attestation processes in order to answer questions such as:

- How many objects have been attested or recertified?
- How are we doing compared to previous attestation or recertification processing?
- How do the various departments compare in their performance?

For example, Identity Manager's attestation dashboard provides charts that enable you to see the status of attestation policies at a glance (see Figure 2).



Attestation Policies

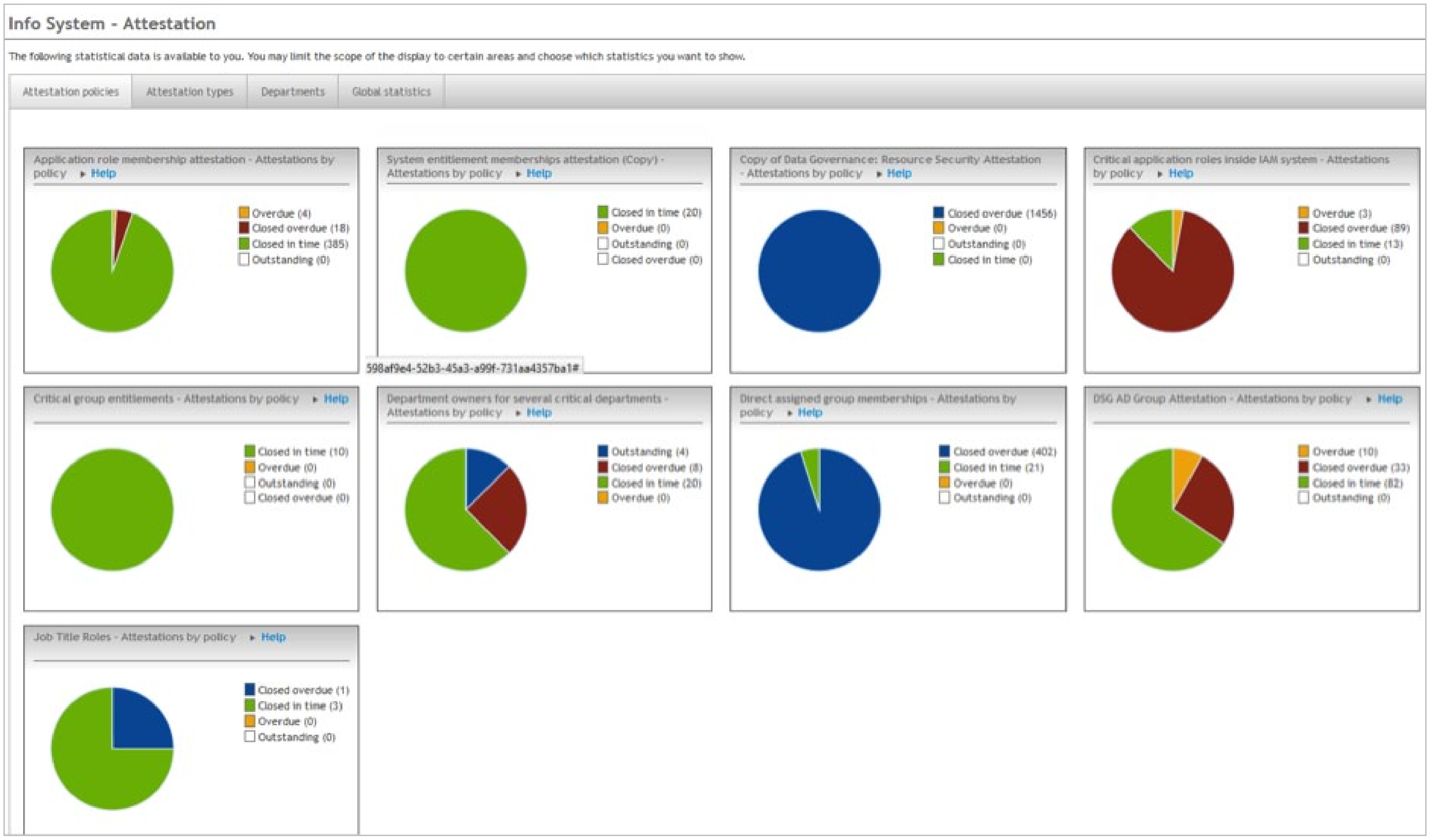
This page displays current and forecast information of pending attestation runs. It also allows you to change the due date of those runs and send reminder e-mails to their attestors.

Min. Category: ○ Good ○ Mediocre ● Bad

	Attestation policy	Start	Due date	Progress	Forecast	Forecast date	Delay	Actions
●	Data Governance: Accounts with direct access attestation	12.03.2013	19.03.2013	62 %	N/A	12.10.2015	937	
●	Attestation of assignments to system entitlements	13.03.2013	20.03.2013	25 %	N/A	26.08.2019	2351	
●	Department attestation	13.03.2013	20.03.2013	36 %	N/A	31.08.2017	1625	
●	Data Governance: Resource classification attestation	13.01.2014	20.01.2014	60 %	N/A	30.04.2015	465	
●	Application role membership attestation	13.01.2014	20.01.2014	98 %	N/A	27.10.2014	280	
●	DSG AD Group Attestation	01.09.2014	08.09.2014	65 %	N/A	20.11.2014	74	
●	Critical application roles inside IAM system	01.10.2014	08.10.2014	0 %	N/A	never	N/A	
●	Data Governance: Resource ownership attestation	01.10.2014	08.10.2014	0 %	N/A	never	N/A	
●	Attestation of business role system entitlement assignment	01.10.2014	08.10.2014	58 %	N/A	08.11.2014	32	
●	Data Governance: Resource security attestation	01.10.2014	08.10.2014	0 %	N/A	never	N/A	

Export this view: PDF | CSV
last loaded: 23.10.2014 13:41:58

Figure 1. Identity Manager's interactive report displays all the information needed by the attester while still providing a clear overview of the recertification process.



Info System - Attestation

The following statistical data is available to you. You may limit the scope of the display to certain areas and choose which statistics you want to show.

Attestation policies
Attestation types
Departments
Global statistics
Application role membership attestation - Attestations by policy ▸ Help
Overdue (4)
Closed overdue (18)
Closed in time (385)
Outstanding (0)
System entitlement memberships attestation (Copy) - Attestations by policy ▸ Help
Closed in time (20)
Overdue (0)
Outstanding (0)
Closed overdue (0)
598af9e4-52b3-45a3-a99f-731aa4357ba1#
Copy of Data Governance: Resource Security Attestation - Attestations by policy ▸ Help
Closed overdue (1456)
Overdue (0)
Outstanding (0)
Closed in time (0)
Critical application roles inside IAM system - Attestations by policy ▸ Help
Overdue (3)
Closed overdue (89)
Closed in time (13)
Outstanding (0)
Critical group entitlements - Attestations by policy ▸ Help
Closed in time (10)
Overdue (0)
Outstanding (0)
Closed overdue (0)
Department owners for several critical departments - Attestations by policy ▸ Help
Outstanding (4)
Closed overdue (8)
Closed in time (20)
Overdue (0)
Direct assigned group memberships - Attestations by policy ▸ Help
Closed overdue (402)
Closed in time (21)
Overdue (0)
Outstanding (0)
DSG AD Group Attestation - Attestations by policy ▸ Help
Overdue (10)
Closed overdue (33)
Closed in time (82)
Outstanding (0)
Job Title Roles - Attestations by policy ▸ Help
Closed overdue (1)
Closed in time (3)
Overdue (0)
Outstanding (0)

Figure 2. Identity Manager's attestation dashboard enables you to see the status of attestation policies at a glance.

Conclusion

Organizations today are increasingly concerned with achieving regulatory compliance and reducing risk. In particular, increased demand for the traceability of IT permissions has organizations seeking higher levels of sophistication in their attestation and recertification methods.

Progressive organizations are adopting a modern attestation and recertification architecture that uses business roles to control permission assignments and includes a dashboard recertification tool that identifies potential issues and facilitates the review process.

About the author

Matthias Bauer has been the manager responsible for the development of Dell One Identity Manager for more than 15 years, in addition to serving as managing director of Dell Software GmbH in Germany.

Matthias studied electrical engineering at the University of Karlsruhe (TH) with a focus on fibre-based communication engineering and was a co-founder of Voelcker Informatik.

Progressive organizations are adopting a modern attestation and recertification architecture that uses business roles to control permission assignments and includes a dashboard recertification tool that identifies potential issues and facilitates the review process.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL’S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.