The Age of Audit:
The Crucial Role of the “4th A” of Identity and Access Management in Provisioning and Compliance

Why Audit is a required element of any successful access provisioning and regulatory compliance
## Table of Contents

1. **Introduction** 3
2. **IAM Overview** 4
3. **Seasons of Identity Management** 5
4. **Audit is required for any successful IAM implementation** 7
5. **Life after the initial implementation** 8
6. **How Consul InSight™ Helps IAM** 9
   6.1. InSight speaks the language of Identity and Access Management 9
   6.2. InSight provides users and data set groupings based on actual access patterns 10
   6.3. InSight facilitates the creation of access policy rules based on your security event data 11
   6.4. InSight provides continuous event and compliance auditing with detailed reporting 12
7. **How Audit Enables Compliance** 13
8. **Conclusion** 14
9. **References and further sources of information** 15
1. Introduction

In today’s security management landscape, enterprises recognize the value of implementing identity and access management (IAM) solutions to administer user authentication and authorization. Most common are solutions that allow for enterprise Provisioning of users. Such solutions help organizations lower user administration costs, improve the security and protection of key corporate applications and information assets, and ensure compliance with the policies of the enterprise and external governing bodies.

With the sudden increase in regulations and standards, there is now recognition that Audit – often regarded as the “4th A” after Administration, Authentication and Authorization – is a particularly vital component of the IAM process. Audit should not simply be the ability to report on the identity database embedded in a traditional Provisioning solution, but rather the ability to independently collect and monitor how users are accessing information.

This white paper will describe the IAM process and how Audit plays a crucial role before, during or after implementation of an access provisioning solution. Using examples from Consul InSight™ Security Manager¹, it will show how the right Audit solution enables large organizations to:

- Baseline users and IT assets
- Benchmark access behavior
- Establish access policy
- Report policy exceptions
- Monitor security breaches
- Archive all log files
- Audit events, users and data

With InSight, Audit becomes a key enabler for Provisioning and Compliance initiatives.

¹ Consul risk management, Inc. and BMC Software, Inc. have collaborated to offer InSight for CONTROL-SA by Consul, a version of InSight available through BMC.
2. IAM Overview

Identity management is the process of managing information for a user’s interaction with an organization. Key identity management functions include adding, updating and deleting user information and permissions for a company’s systems, applications and data stores. In general, identity management is thought of as encompassing four A’s (source: Gartner, Forrester)

- **Authentication**: Enterprises must ensure that users are properly identified and that these identities are validated to IT resources.
- **Authorization**: Enterprises must know that users can access only what their job function allows them to access within the enterprise.
- **Administration**: Enterprises must have a consolidated, enterprise-wide view and a way to manage user access.
- **Audit**: Enterprises must ensure that the activities associated with user access (administration and real-time enforcement) are logged for day-to-day monitoring, regulatory and investigative purposes.

While there are many reasons why enterprises implement a comprehensive IAM solution, there are three key benefits that stand above the rest.

**First**, enterprises are able to lower user administration and provisioning costs with an IAM solution. They are able to achieve this by automating manual or semi-manual tasks involved in changing access rights, provisioning end users, and eliminating duplicated tasks and reducing the risk of error. This approach will enable the IT staff to focus on core functions, easily scaling administration to the number of users.

**Second**, enterprises are able to improve the security and protection of key corporate applications and information assets. IAM provides a centralized, authoritative source of user identities, privileges and access information. This offers the enterprise real-time permission and policy enforcement, continuous real-time auditing to detect and remove security risks, and the ability to easily and automatically remove terminated users and revoke their access rights.

**Lastly**, IAM allows enterprises to accelerate compliance against their own internal security policies and external regulations such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) or Basel II. Companies today face a landslide of regulations that require everything from strict data controls to extensive record keeping and auditing to demonstrate compliance. Implementing measurable
access security policies and intelligently archiving and auditing vast amounts of security event information to demonstrate compliance are no longer optional.

3. Seasons of Identity Management

While the benefits of IAM are clear and potentially substantial, they do not come without challenges. In fact, the specific challenges will depend on your IAM “season.”

Before you decide to adopt IAM, you are in IAM “winter.” You have little visibility into who is doing what. Access rights management is balkanized, potentially leaving gaps and inconsistencies. You are never completely certain if the right people have access to the right data. Worse, you are not certain if the wrong people have access to critical data. Additionally, you have several challenges selling management on the investment. Cost savings may be hard to quantify since the benefits may be reaped across many departments. IAM is a long-term investment with a break-even point more than a year out. Many companies are averse to taking on long payback projects. The benefits of improved security and administration processes may be undervalued, making costs difficult to justify. Probably the biggest hurdle is the belief that the current approach to system and user administration is “good enough.”

Once you make the decision to implement IAM and start the implementation, you are in IAM “spring.” You look forward to reaping all the benefits of IAM, and you have all of the hope, optimism and enthusiasm of springtime.

However, enterprises are then hit with the complexity of the installation - IAM “summer.” You may find IAM technologies difficult and expensive to integrate within your existing infrastructure. You realize that you need to understand your current workflows and data architecture. When you realize that you do not have a way to easily gather this information, you are overwhelmed. You start to feel the “summer heat” and ask, “Where do I start?”

“Autumn” follows when your IAM solution is in place and you are managing your operational IAM environment. The summer heat is gone and you are reaping the initial benefits. You begin to consider that IAM can help you improve your security and information protection mechanisms and accelerate compliance with internal policies and external regulations. You start to ask, “Are the right controls in place?” and “Are my controls effective?”
So, which season is the biggest challenge? Like many things in life, the biggest challenge is taking the first step. For example, many of you have been through a decision to change some aspect of your daily routines. You determine that you want to start going to the gym more often, start to run regularly or start to read more. Deciding to go to the gym more regularly is easy. The hard part is deciding which gym, what types of exercise, how often and what time of day. All of these decisions, particularly if you have the daunting task of gathering data to make the decision, can paralyze you to the point of inactivity. This is the same for IAM. The hardest part is getting started. So, how should you get started?
4. Audit is required for any successful IAM implementation

In many instances, the biggest obstacle to your initial deployment is the lack of data. You must establish an information access baseline. You need to understand your current workflows and your data architecture - Who should access which data? Who is actually touching the data? When, where and how are they accessing the data? This entails identifying your users and IT assets and establishing a baseline for access behavior across your enterprise. This baseline is the first step towards understanding roles, groups and profiles in your environment, providing you with the information you need to establish your initial access policies, including roles, groups and authorities.

Much of this information is already available in audit logs across your enterprise. The challenge is collecting and storing the information, making sense of it, and then making intelligent decisions based on it. How do you do this?

<table>
<thead>
<tr>
<th>Collect</th>
<th>You need secure and scalable log collection, to consolidate, and archive for a wide variety of platforms – mainframe to appliance, operating systems, security devices, applications, databases.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translate</td>
<td>You need a strong, business oriented, technology-independent normalization method that translates cryptic logs into the same language you speak when considering roles, groups and profiles for an IAM implementation - Who, touched What, When, Where, Where to, Where from, and on What.</td>
</tr>
<tr>
<td>Analyze</td>
<td>You need to leverage the collected log files to help to determine logical groups, roles and profiles based on actual access patterns. Grouping templates provides a simple and effective way to organize people, assets and data into common groups.</td>
</tr>
<tr>
<td>Baseline</td>
<td>You then need to establish your baseline. That is, define access policy rules based on security event data and proposed groupings.</td>
</tr>
</tbody>
</table>
5. Life after the initial implementation

Once your IAM system is in place, the same audit tools and audit process moves you into the next level of identity management implementation—leveraging roles and profiles to improve overall security and accelerate regulatory compliance. What are some of the ways an audit solution can improve security and accelerate compliance?

<table>
<thead>
<tr>
<th>Improve access policies</th>
<th>Audit events, users and data and filter collected information against security policy. Policy breaches might indicate where too much access is provided; logon failures might indicate where more access is needed. You can adjust your profiles accordingly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve forensic investigations</td>
<td>Perform automated, ongoing monitoring of breaches to policy, with the ability to conduct detailed forensic audits.</td>
</tr>
<tr>
<td>Facilitate actionable audit</td>
<td>Act upon severe breaches to policy by disabling the account user ID or enterprise user definition of the person committing the policy breach.</td>
</tr>
<tr>
<td>Provide customized reporting for all levels of the organization</td>
<td>Provide reporting tailored to specific regulations and the needs of security operations and auditors. You also need reports that facilitate easy event auditing and demonstrate policy compliance.</td>
</tr>
</tbody>
</table>
6. How Consul InSight™ Helps IAM

6.1. InSight speaks the language of Identity and Access Management

Many security vendors speak about “event anomaly,” “IP packets,” “signatures” and other technical terms. InSight speaks about security events more clearly in a “language” we call the W7 language. All logs are normalized to easily inform you of Who, touched What, When, Where, Where to, Where from, and on What. This is the same language you speak when considering roles, groups and profiles for an IAM implementation. InSight is able to turn cryptic logs into W7 information.
6.2. InSight provides users and data set groupings based on actual access patterns

InSight’s user and data classification templates provide standard and regulatory relevant groups for each of the 7 W’s: e.g., Who groups, What groups, etc. These templates provide a starting point that can be customized to any business environment and enable you to group your organizational assets into business relevant categories from which to report. These groupings can be consistent with the groups and profiles you use in your IAM efforts. With InSight, the security manager is now able to establish access roles and groups based on the enterprise’s actual access patterns.
6.3. InSight facilitates the creation of access policy rules based on your security event data

Once the data is normalized and placed in business relevant groups based on actual access patterns, InSight is able to help create an access policy. InSight’s policy templates provide default access policies relevant to either an industry standard, such as ISO 17799, or a regulation such as SOX or HIPAA. By reviewing your actual security event data against InSight’s policy engine, you are able to create a set of simple rules that are implemented in an operational W7 access policy. In other words, with InSight you go from cryptic logs, to event auditing and monitoring with logical groups, to an access policy that is a jump-start for your IAM implementation.
6.4. InSight provides continuous event and compliance auditing with detailed reporting

Finally, having used the data from the log files to establish logical access groups and policies, you can use InSight to monitor your entire network. Below you see InSight’s compliance dashboard. The compliance dashboard provides an easy-to-understand, color-coded matrix highlighting levels of compliance based on user behavior and data access. The dashboard also contains a variance chart that measures policy violations versus goals over time.

When your analysis and review indicate that you need more detail, InSight provides the ability to drill down from the compliance dashboard to detailed reports on who violated your access policy and how. There are more than one hundred different reports available to enable easy event auditing and policy compliance. These reports can serve as a feedback mechanism on your IAM implementation: breaches might indicate where too much access is provided; logon failures might indicate where more access is needed. You can adjust your profiles accordingly.
7. How Audit Enables Compliance

Audit should enable compliance by monitoring who is touching which files and compare that against set policy. For HIPAA, this means monitoring who touches patient data; for Sarbanes-Oxley, who touches financial information; for Gramm-Bleach Bliley and the CA-SB 1386, who touches customer information. For each and every regulation InSight provides the access audit perspective required by law. Most importantly, InSight does this by comparing Who should be allowed to touch What (Policy) with Who does What (logs):

A comprehensive Audit solution like InSight enables compliance by allowing organizations to:

**Implement procedures:**
- Implement security policy
- Employ ISO17799 for compliance
- Prepare for stringent security audits

**Measure compliance:**
- View compliance dashboard
- Print best-practice reports
- Track policy exceptions over time

**Understand who touches what:**
- Monitor user behavior
- Audit file access
- Track compliance breaches

**Manage security events:**
- Correlate disparate security devices
- Manage diverse platform events
- Consolidate and archive native logs
8. Conclusion

IAM’s benefits are clear but with a significant set of challenges. The biggest challenge is getting started. Auditing and creating an information access baseline provides the most effective way to understand users, assets and user behavior toward those assets. Then you can proceed from cryptic logs, to event auditing and monitoring with logical groups, to an information access policy that is a jump-start for your IAM implementation. With this approach, you will be able to document access behavior based on actual security event data, group users and data based on access patterns, and define access policy rules based on security event data and proposed groupings. By improving implementation time, you can improve your overall security infrastructure, accelerate regulatory compliance or internal audit efforts and achieve ROI faster.
9. References and further sources of information

URL: www.gartner.com

**PricewaterhouseCoopers** – “Identity Management - The business context of security: a white paper.”
URL: www.pwc.com/extweb/service.nsf/docid/83ACF0A4CAB036C685256C6A0055D964

URL: www.forrester.com

Further information about Consul Insight is also available. Consul InSight™ is developed, sold and supported by:

**Consul risk management, Inc**
Suite 205
2121 Cooperative Way
Herndon, VA 20171
USA
Telephone: +1 800 258 5077
Email: contactsales@consul.com

www.consul.com