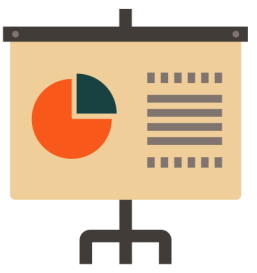
Chapter 4

Intelligent IAM for Dummies

9 THINGS

TO LOOK FOR IN AN INTELLIGENT IAM SYSTEM

1. Risk Analytics



An IIAM system's strength lies in its capability to show you what risks your organization is facing. You should look for a system that can apply big data analysis techniques to help find the problems you're most worried about before they cause real issues.

2. Alerting Capabilities

Your IIAM system is only as effective as its capability to tell you when something is wrong. Look for an IIAM system that can alert you in ways that fit your business process and preferences.

3. Support for Role Changes

When a user's role changes, her rights need to change, too. A good IIAM system should handle when a user's role changes, or if she's terminated, by ensuring that the appropriate rights are removed for that user.

4. Intelligent Provisioning

Linking an IIAM system to your provisioning system should allow you to score the risks that an access request creates and create workflows based on how much scrutiny an access request needs.

5. Privileged Account Monitoring

Privileged accounts,such as those that belong to system administrators, need to be watched closely for both abuse and for inadvertent growth in rights and privileges.

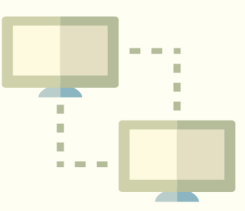
6. Strong Visualization Capabilities

The complex interactions between user accounts and their rights can make finding problems a tedious process of reading error logs and configuration information line by line. Strong visualization capabilities make finding problems and detecting anomalies something you can do at a glance.

7. Continuous Governance

The gap between when users are given rights and when those rights are audited is the time that organizations face the most risk. Micro-certification can help by providing immediate review as needed by managers, which ensures that they see and address problems directly.

8. Access Rights Monitoring



Polls show that excessive developer access rights are a concern for many organizations. Tracking what access individuals have compared to what they really need is a key feature for any IIAM system.

9. Identification of Segregation of Duty Issues

Separating the rights that are required to perform sensitive actions is important, and accounts that end up with too many rights may be able to bypass that. Automated detection is important to prove to yourself and auditors that your separation of duties works.

CORE SECURITY