Bell Integration

TRANSACT
TRANSFORM
RUN
RECYCLE

Choose The Right Identity & Access Management Solution

Realise business value by protecting critical assets from unauthorised access

Helping you to secure an extended enterprise

At the core of every cyber-security strategy is identity and access management. Because so many security issues and audit failures are user-related, organisations need to make sure people have appropriate, up-to-date access entitlements and that their access activities are monitored wherever they are located.

In today's open enterprise, users can be the weakest link in security. To combat these insider threats and protect critical assets, organisations need automated, role-based access controls that can help identify who the users are, where they are located, what they want to do, and what their normal behaviour is before letting them in the door.

In fact, organisations now need "threat-aware" identity and access management (IAM) solutions to help them. To help you evaluate whether an IAM solution effectively supports your short- and long-term objectives, this guide includes checklists of key features and capabilities in the following areas:

IAM key features and capabilities:

- ➔ Identity governance and management
- ➔ Access management for web, cloud and mobile environments
- ➔ Policy-based entitlements and access controls
- ➔ Identity intelligence (for monitoring and auditing)
- ➔ Time to value

To help you evaluate whether an IAM solution effectively supports your short- and long-term objectives, this guide includes checklists of key features and capabilities.

Identity governance and management

Evolving threats and security breaches are forcing organisations to reconsider their approach to user and access management. As regulations and compliance efforts focus more and more on how and why user access is granted, organisations need to ensure their identity management practices comply with external and internal security policies and requirements.

Identity governance and management is the evolution of core identity management functions. While traditional identity management focuses on IT processes, such as user provisioning and authorisation, identity governance goes much further to address the business requirements of compliance managers, auditors and risk managers.

Identity governance and management solutions help organisations protect identity as a new perimeter with controls to manage, enforce, and monitor user entitlements and access activities. With identity governance, organisations can help protect their critical data that is vital to business survival and success. They can define, discover, validate and maintain truly meaningful business roles. And based on those business roles, they can maintain strong control over user access to applications and carefully monitor how the entitlements align with business roles and responsibilities.

Centralised, automated identity management solutions can make administering and auditing user roles, identities, credentials and access permissions more efficient and accurate. An automated, policy-based provisioning system can support adherence to your business policies, provide proper context for securing user access and enhance regulatory compliance. An easy-to-use solution that empowers business managers to make entitlement decisions for their employees can help ensure that all users have access privileges appropriate for their business role.

Managing and governing user identities and access privileges is instrumental in maintaining regulatory compliance and reducing risk. The right identity governance and management solutions should help organisations create an identity governance strategy, centralise identity management tasks and reduce related costs. The products should also help audit, monitor and report on user compliance with acceptable use policies.

An easy-to-use solution that empowers business managers to make entitlement decisions for their employees.

Identity governance and management

To help you evaluate whether an IAM solution effectively supports your short- and long-term objectives, we've created a checklists of key features and capabilities that will allow you to benchmark your existing systems and processes against the latest security technology.

Does your exisiting solution do the following:	Yes	No
Provides complete user lifecycle management, password management and role governance in a single integrated solution		
Creates comprehensive identity governance, risk and compliance infrastructure such as audits, reporting, access review and certifications, separation of duties (SoD), and access risk mitigation		
Helps reduce risk with zero-day deprovisioning of users when they leave the organisation or change roles		
Improves collaboration with business users by aligning roles design with business objectives		
Facilitates continuous development and optimisation of roles as business processes evolve		
Defines user roles from a business-activity point of view—rather than application capabilities—and aligns the roles with business policies		
Simplifies the design, implementation and validation of role and access structures across the organisation, performing role mining and role optimisation with SoD validation		
Manages and prevents business process conflicts through group management and SoD enforcement		
Provides a business-friendly, intuitive user interface to support business managers requesting and approving access for their employees, both on-premises and via a mobile device		
Empowers users to actively participate in and manage their own access privileges and passwords,helping reduce costs		
Helps enforce pre-established policies for how user access should be granted throughout access request and provisioning processes		
Supports the ability to create and implement actionable business-centric governance rules for quick time to value		
Provides a self-service interface for user enrollments, user validation, account updates and password management		
Reduces costs and simplifies deployment with a virtual appliance format		
Supports identity management on a group basis, simplifying and reducing the cost of user administration		
Bundles a best-of-breed directory with data integration and synchronisation tools to help solve integration challenges		
Reconciles accounts automatically and on demand to rapidly and reliably discover invalid "orphaned" accounts and unnecessary entitlements, and to initiate either automatic or manual remediation processes		
Maintains accurate records of configuration and changes to user access rights for auditing purposes		
Provides access to both approval and operational workflows, allowing customisation of the provisioning activity		
Integrates with a wide range of identity servers, applications, middleware, operating systems and platforms, including SAP and Oracle		
Addresses compliance mandates via audit trail collection, correlation and reporting		
Helps reduce the time and effort needed to design, manage and approve roles and role structures for enterprise IT governance		
Provides a layer of analytics for greater visibility and risk prioritisation		

Directory services

Does your exisiting solution do the following:	Yes	No
Serves as the identity data foundation for web applications and identity management initiatives		
Offers a universal directory capability, to transform identity silos and support "virtual directory"-like deployments		
Offers in-depth user insight via security intelligence platform integration, a lightweight directory access protocol (LDAP) group connector and analytics platform reporting		
Includes a System for Cross-domain Integration Management (SCIM) connector for enhanced on-boarding to cloud applications and other SCIM-enablement targets		
Easily synchronises with other directories to provide a single, authoritative, enterprise-level view of data		
Provides a highly scalable identity infrastructure to meet the needs of all organisations, from small and midsized businesses to those with hundreds of millions of users		
Offers intelligent search and social networking support for identity store browsing		

Privileged identity management

Does your exisiting solution do the following:	Yes	No
Provides complete identity management for authorising privileged users throughout the users' lifecycles		
Enables the secure setup, management and approval of a pool of shared and privileged accounts to help improve control and oversight of privileged identities		
Provides an integrated approach to managing both privileged and non-privileged identities for simplified IT deployment and ease of use		
Provides out-of-the-box connectors to support a wide variety of managed endpoints such as servers, applications and devices		
Helps secure and track the use of privileged credentials in applications, and supports password rotation of those credentials		
Allows you to schedule password changes in managed application instances using lifecycle rules		
Helps reduce total cost of ownership and speeds time to value with a virtual appliance deployment option		
Provides privileged user accountability with optional session recording/replay support and usage tracking of shared IDs		
Protects privileged access to enterprise resources with secured user credentials, automated password management and single sign-on capabilities		
Strengthens compliance and governance with comprehensive tracking and reporting of privileged users' activities		
Supports external directories such as Microsoft Active Directory for user authentication, eliminating the need for a separate, dedicated directory		
Enables control and auditing of privileged access to cloud-based resources		

Access management for web, cloud and mobile environments

Many organisations face access management chaos. As applications and resources have spread across on-premises data centers and multiple cloud providers, users are accessing these resources from anywhere and on multiple devices. These trends have left many access management systems fragmented and access polices inconsistent. In addition, the fragmented environments are expensive to maintain and challenging to secure.

Organisations can take back control of access management by using an integrated solution to manage access across many common scenarios. For example, combining web application protection, single sign-on, risk-based access control and identity federation is an efficient, effective approach to securing web, mobile and cloud workloads.

Access management for web, mobile and cloud environments

Does your exisiting solution do the following:	Yes	No
Enables secure user access to web, mobile and cloud applications with single sign-on, session management and context-based access control		
Provides an integrated solution to safeguard user access to web, mobile and cloud workloads		
Supports multiple standards for cross-site authentication, including Security Assurance Markup Language (SAML), Open Authorisation (OAuth), Liberty Alliance and Web Services Federation Language (WS-Federation) token-passing protocols		
Provides integrated access management with a web reverse proxy for use across the enterprise		
Simplifies setup and maintenance with local management graphical user interface (GUI) and automated service updates		
Helps protect user access and applications with integrated threat intelligence and built-in protection against application threats		
Enforces context-aware user authorisation and authentication using information about the user, device fingerprinting, one-time passwords, geographic location awareness, fraud indicators and IP reputation scores		
Provides a graphical policy management interface that supports authoring complex access control policies		
Integrates with existing identity management systems to import users and roles and synchronise passwords between the two products for efficient user lifecycle management		
Provides identity services to validate and centrally manage access across private, public and hybrid cloud deployments		
Supports federated single sign-on for users across multiple cloud-based applications through support of SAML 2.0 and OpenID Connect protocols for federated access		
Simplifies installation and maintenance with an easy-to-deploy-and-manage physical appliance or virtual appliances		

Does your exisiting solution do the following:	Yes	No
Delivers built-in Layer 7 load balancing and distributed session caching to provide shared session management across multiple appliances and application instances		
Provides mobile sign-on, session management and an authentication service for supporting multiple strong authentication schemes		
Provides flexible web and identity services using its own security token service (STS) to validate and issue a wide variety of identity formats		
Helps block the Open Web Application Security Project (OWASP) top 10 web vulnerabilities before they reach the targeted application		
Offers high performance and scales to tens of millions of users and hundreds of applications		
Provides the ability to securely implement “bring your own identity” scenarios using popular social identity providers		
Includes pre-integrated federation connectors to popular cloud applications		
Centrally manages user access to on- and off-premises cloud and web applications services in heterogeneous IT environments		
Supports broad and flexible integration with strong third-party authentication solutions		
Offers mobile access control policies that integrate with mobile device management, application development and malware detection solutions		
Provides risk-based and multi-factor authentication capabilities to protect assets depending on the risk context		

Many access management systems are fragmented and access polices inconsistent.

Policy-based entitlements and access controls

As the number of users increases exponentially, organisations need an efficient solution to help them consistently manage and enforce access-control policies across every application, data source, operating system and organisational boundary.

These policies must integrate with core business systems and keep identity information synchronised across multiple sources. Organisations must be able to put into place access-control policies that reflect business goals and help ensure regulatory compliance—and do both in a cost-effective manner. Also, as organisations establish their access control policies, they need identity and access management tools that include analytics to help identify and mitigate risks.

Policy-based entitlements and access controls

Does your exisiting solution do the following:	Yes	No
Provides a business-friendly description of what users can do with their access rights for better decision making in new access-approval requests, recertification and audit reviews		
Enables managers to proactively enforce pre-established business policies for how access should be granted throughout the access request and provisioning processes		
Enables modeling of security policies and creating of security-policy templates for consistent use across the organisation		
Allows application owners to create data entitlements using roles and attributes without requiring knowledge of IT operations		
Provides auditing, tracking and reporting of user access and entitlements for actionable IT operations and effective compliance reporting		
Includes what-if policy change simulation analysis to identify who and what entitlements will be impacted before a change is made; provides an impact analysis and preview of policy changes, with ability to drill down on accounts, attributes and values		
Incorporates business rules into access-control decisions and evaluates these rules dynamically at run-time		
Manages and prevents business process conflicts through group management and SoD enforcement		
Provides a policy-based user authentication and authorisation system that helps defend against the latest web-based security threats		
Periodically reviews and recertifies user access, identifying SoD policy violations and remediating risks associated with inappropriate user access privileges		
Sets an access policy that automatically detects and remediates intentional and inadvertent noncompliance events in real time		
Automatically escalates and redirects workflow processes to alternate participants when timely action is not taken		
Scales to tens of millions of users for authentication and authorisation		
Enables multiple policy enforcement points for application and data sources such as Microsoft SharePoint, IBM® DB2® and other application and data resources		
Uses the security token service (STS) to validate and issue a wide variety of identity formats and to flow auditable identities between applications and services across multiple security domains and the organisation		

Identity intelligence

Organisations must not only be able to control access to data and applications, but also to demonstrate the strength and consistency of their access controls throughout the identity lifecycle and provide auditable proof of compliance.

In today's complex computing environments, organisations need a closed loop view of who has access to what, why they have access to it, and what they are doing with that access. This visibility must extend to privileged and trusted users, as these accounts are particularly vulnerable to abuse.

The open enterprise needs to be able to quickly detect anomalous user behavior. It needs to be able to analyse actions to discover—and fix—system vulnerabilities as well as help prevent malicious activities in the future. Monitoring reports can be used to understand whether user activities align with the rights and policies of the organisation. Any abnormal or out-of-policy activity should be highlighted so it can be addressed and corrected, including monitoring, as part of the overall compliance process closes the loop and helps ensure that the right level of security is in place.

Identity intelligence

Does your exisiting solution do the following:	Yes	No
Provides risk-based compliance and threat analytics for improved ability to combat insider threats		
Produces customisable analytics reports that show role details, user access, permission views and explorations of modeling data		
Integrates with security information and event management (SIEM) tools such as IBM QRadar® Security Intelligence Platform or other reporting tools to provide actionable insights for reducing risks and demonstrating compliance		
Supports a comprehensive risk management program, which can impact the organisation's financial position and security compliance posture		
Utilises a single, secure identity repository from which virtually all identity events can be tracked and audited		
Provides true closed-loop policy compliance enforcement that both detects and remediates access entitlements granted outside the provisioning process		
Provides a single identity graphical user interface for performing administrative functions and for tracking and auditing identity events		
Includes workflows as an integral component so that all lifecycle and provisioning events are managed and monitored by the solution, which can then log all transactional data for forensic auditing and reporting		
Offers closed-loop access and audit management support for integrating with security information and event management tools		
Transparently logs all user login activities and centrally records them inside the system database to support compliance		
Translates and maps a diverse set of user identities across different services		

Does your exisiting solution do the following:	Yes	No
Establishes an identity trust management framework to help ensure transactions are performed securely		
Tracks and collates all login events, allowing users to extensively audit application access and generate detailed reports		
Provides an audit trail of who has access to what and who approved those access rights		
Offers privileged user monitoring, reporting and auditing on databases, applications, servers and mainframes		
Translates captured native log data into easy-to-understand reporting that can be used without the need for any platform knowledge		
Updates administrators with IAM analytics and reporting for improved visibility into potential risks		
Provides an easy-to-use interface for creating custom reports, including summary, detail and threshold reporting		
Supplies fine-grained logging and reporting of user activities that can help demonstrate compliance with government security regulations		
Provides comprehensive tracking and reporting on how privileged identities are used and what users have done with these identities		

Time to value

As you're evaluating different identity and access management solutions, it's important to select one that offers rapid time to value and the ability to add new capabilities, such as identity governance, fraud protection or reporting tools, as needed.

The right solution, while cost effective, should also include a number of key features designed to provide easy configuration, integration, maintenance and robust security—especially in complex enterprise environments.

Time to value

Does your exisiting solution do the following:	Yes	No
Provides an integrated IAM solution to simplify the ongoing management of disparate security systems across the extended enterprise		
Includes necessary infrastructure adapters, leading commercial versions of middleware and software components (including necessary databases), LDAP servers, and web and application servers		
Delivers user metrics to support collaboration among business, IT and audit teams		
Provides access management solutions in hardware or virtual appliance formats for simplified configuration and faster time to value		
Supports integration with third-party applications (including SAP, Oracle and Microsoft), as well as support for multiple directories and user repositories and heterogeneous middleware		
Supports local languages and incorporates dynamic language support to display deployment-specific content in each user's preferred language		
Provides breadth of platform support, including Microsoft Windows, Linux and IBM z/OS®		
Helps secure access to applications and workloads, including web, mobile, cloud, and application programming interfaces (APIs), with a single integrated appliance		
Simplifies the user experience with single sign-on access across applications, wherever they are running		
Provides visibility into risks to help cross-functional teams govern identities, gain control and support regulatory compliance		

Next Steps

This is a lot to take in and maybe it has raised issues that you hadn't considered or have the technical resources in house to address.

To find out how you can ensure your Identity and Access Management meets your business needs through compliance and risk reduction, simply drop us an email using the link below and one of the team will be in touch to set up a simple review to discuss any questions you have.

See how Bell Integration can help your business succeed. Please contact us on

enquiries@bell-integration.com
or visit www.bell-integration.com