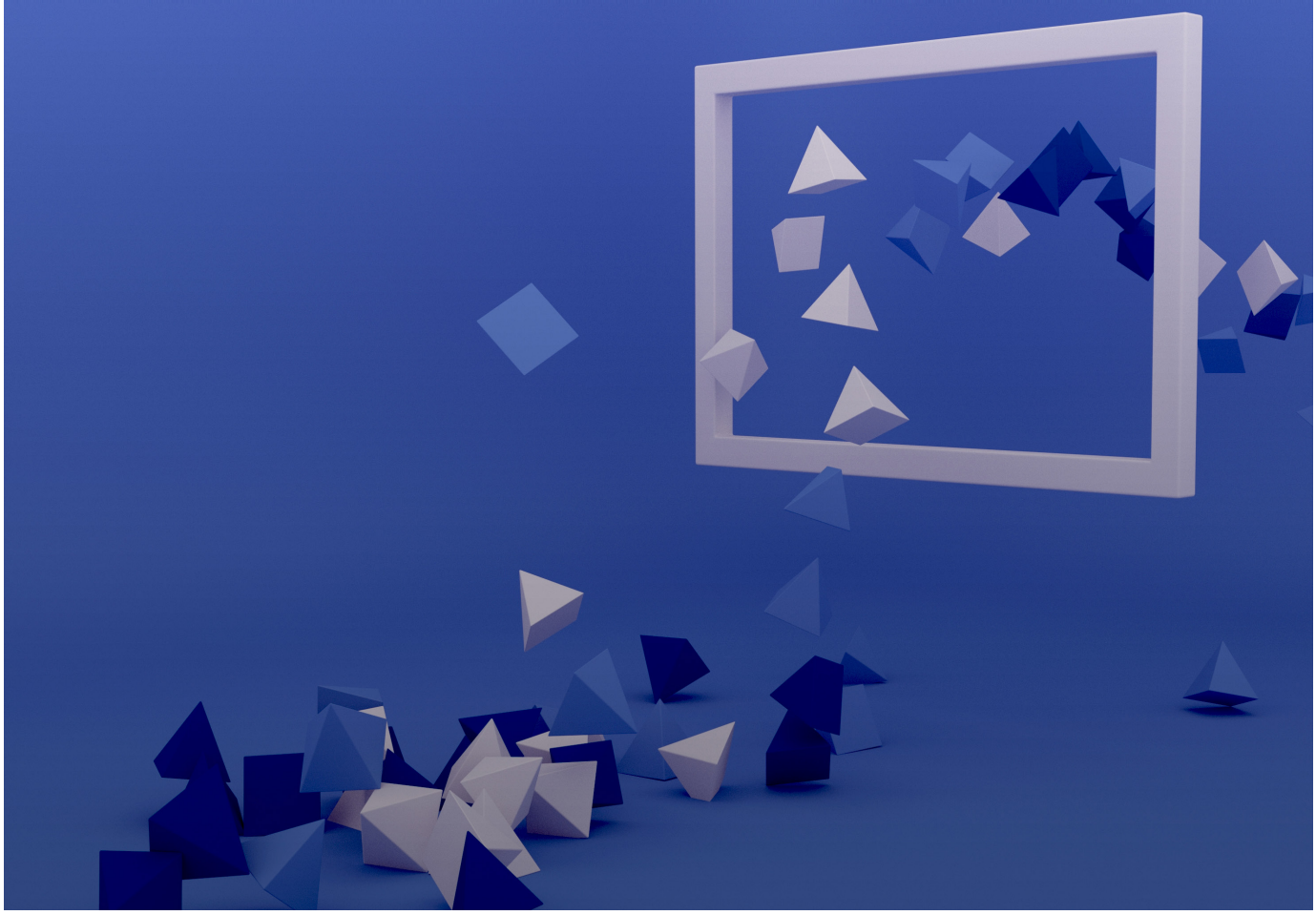
AUJAS CYBERSECURITY
An NSEIT Company

aujas.com

Rapid Application Onboarding: Best Practices

WHITEPAPER | IDENTITY & ACCESS MANAGEMENT



Abstract

This whitepaper delves into best practices of rapid application onboarding. It explains organizational, procedural, and technical tools that enable rapid onboarding best practices for organizations looking to onboard hundreds of business applications to an identity and access management (IAM) system. Additionally, the paper discusses the benefits, challenges, and key considerations associated with lifecycle management, separation of duties (SoD) policies, and role-based access control (RBAC).

Introduction: why is rapid onboarding necessary?

Businesses invest in IAM technologies for two primary reasons: cybersecurity benefits and cost savings. A properly configured IAM solution does more than just enforce cybersecurity best practices such as least privileges, access certifications, and separation of duties (SoD) policies. It automates complex and time-consuming human tasks, such as new account creation, access requests, and de-provisioning access on an employee's last day. IAM technologies present a huge opportunity for organizations because they lie at the intersection of security and automation – yet configuring them properly is a challenge for many businesses.

Organizations are facing never-seen-before challenges when it comes to managing their "digital identities." For many organizations, digital identities span across cloud and on-prem business applications. The business applications used by a typical organization have a wide bell curve in their IAM capabilities – some are cloud-native with SCIM 2.0 integrations, whereas others are legacy RACF servers that run mission-critical programs. The IAM system needs to be able to connect to and protect all these systems.

Rapid application onboarding: best practices

Procedural: Actions companies can take to facilitate application onboarding.

- **Clear communication**

  There is an interdependence between the IAM onboarding team and the application teams. Application teams should receive clear communication from their leadership explaining that the app they support will be onboarded to the IAM system. A timeline and expectation of the work to come should be given in that communication.

- **Top-down approach**

  As application teams are extremely busy, prioritizing one thing (an IAM integration) may mean deprioritizing something else (a feature request). By setting expectations, leadership can ensure that IAM onboarding is a high priority for each application team, preventing confusion and delays.

- **Bottom-up approach**

  Application teams should be supported the whole way. The IAM onboarding team should host "office hours," where application teams can ask questions.

Organizational: Organizational tools that help with application onboarding.

- **Standardized requirements template**

  A standardized requirements template ensures consistency throughout the requirements gathering process. This template will allow application teams to understand the information they need to provide. Post requirements gathering, this template will ensure that developers working on the onboarding will have a clear roadmap for how to proceed.

- **"Scrumban" approach**

  Each application being onboarded should have its own card on a kanban board. The card should be moved through various columns - from requirements to development, testing, validation and completion. There should be a daily scrum where progress is reviewed and issues are flagged. Production deployments should occur in an agile fashion, with additional applications being deployed every three weeks.

- **Katana framework**

  The Katana framework is a template, which Aujas Cybersecurity has developed for application onboarding. It combines various factors, including an application's business criticality, risk, and technical ease of integration. Katana helps to prioritize which applications should be placed in each sprint.

Technical: Software tools that serve as technical enablers.

- **PALM (Platform for Access Lifecycle Management)**

  PALM is a tool developed by Aujas Cybersecurity that allows for rapid application onboarding. It is a centralized website that can prefill data via a CMDB connection, send requirements gathering questionnaires to application teams, enable collaboration, auto-generate documentation, and integrate with various IAM tools for automatic application configuration.

- **Kanban board**

  Kanban boards allow cards to be made for each application to be onboarded. The columns can be organized into various swim lanes, such as "backlog," "requirements gathering," "development," "testing," "validation," and "complete." Kanban cards are updated daily, so the whole project team always knows the status of all applications.

Understanding common pitfalls

1

Lack of clarity on priorities

Integrations with the IAM system is just one of many tasks that application teams are charged with. This often leads to a power struggle between various competing project teams. The only resolution to this is for leadership to clearly explain priorities and set deadlines for the IAM onboarding effort.

2

Confusion surrounding objective

Connecting and IAM system to an application is often relatively low effort but enhancing that connection (i.e. setting up RBAC) is more time intensive. The project team must have explicit goals and the ability to turn down “scope creep” requests.

3

Trying to do everything yourself

IAM vendors and cybersecurity experts like Aujas Cybersecurity regularly onboard hundreds of applications, but for most clients it is the first time they have done it. Companies should ensure that they partner with their vendor and Aujas Cybersecurity so knowledge can be shared by partners who have done this work many times.

Answering a key question – what should be in scope for this project?

When undertaking a project to onboard hundreds of applications, a crucial decision that needs to be made is: “what functionality should be included for the initial production to go live?” IAM solutions offer numerous capabilities, such as RBAC, lifecycle event integrations, policy enforcement, reporting, and more.

Best practice – take a “crawl, walk, run” approach. When doing mass application onboarding, focus on the essentials: connecting to the application, regularly aggregating all accounts and their entitlements, connecting those accounts to the correct digital identity, and removing access from employees who change departments (“mover”) or are terminated (“leaver”).

RBAC, policy definitions, and custom report creation are time-consuming activities. It is therefore a bad idea to include these items in the initial scope as it slows the throughput of application onboarding.

> “An IAM system is only worth the number of applications it is connected to.”

There is a much higher value in an IAM system connected to 1,000 applications that do “leaver” for all of them (removes access for terminated employees) than an IAM system that has fully automated all lifecycle events for 50 applications (but 950 applications are not yet onboarded).

The key questions to ask:

- **What compliance objectives are we governed by?**

  Compliance drives scope. If SOX regulates the organization, biannual access reviews for applications will be mandatory. For CMMC-governed organizations, controls monitoring an identity's access level and citizenship are essential.

- **Should single sign-on and multifactor authentication be implemented?**

  Generally, yes. Single sign-on with multifactor authentication is excellent for security and customer satisfaction. Employees generally prefer single sign-on because of its convenience as they do not need to remember dozens of passwords.

- **Should joiner lifecycle events be in scope?**

  Account creation often has complex requirements. An application should only be part of the joiner process if all employees need an account for that application.

- **Should mover lifecycle events be in scope?**

  Generally, yes. It is best practice to have an individualized access certification when an identity changes the departments/roles. This ensures least privileges and helps to fight against access from "ballooning."

- **Should leaver lifecycle events be in scope?**

  Almost always. Deactivating accounts and removing access from terminated employees is an important security control.

- **Should RBAC be included?**

  Generally, no. Access needs are often different for every application, which results in complex requirements. Any roles created should have simple requirements and should be needed by a large percentage of the organization.

- **What policies/reporting should be in scope?**

  Much like RBAC, each application team's reporting and policy needs are different. For the initial production to go live, policies and reporting requirements should be limited to just what is required to meet organization-wide needs and compliance requirements.

All objectives set in the initial scope should have a high security value, quick return on investment, and help meet the organization's compliance objectives. Once the application is onboarded, there should be a separate "enhancements" team that application teams can work with for specific asks, such as customized reporting or RBAC.

Conclusion and recommendations

In conclusion, rapid application onboarding is a complex but worthwhile investment. It is a prerequisite step for many security best practices. Reporting, SoD policies, access certifications, and automated deprovisioning all rely on a unified digital identity. Clients looking to learn more about best practices and strategies should reach out to Aujas Cybersecurity.

About **Aujas Cybersecurity**

Aujas Cybersecurity -An NSEIT Company empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: