online

IAM Controls Compliance Lifecycle

- Dan Legault, IAM Consultant

In general, efficient implementation of security measures always starts from the definition of policies and procedures enforced downward. With all the highly publicized news headlines of hacking exploits, this exercise should be a mandatory stream of work at the onset of all projects. For the purposes of this piece however, we're going to be talking about it in in the context of Identity and Access Management (IAM) projects.

In the course of working with hundreds of clients over the years, we've found that most organizations lack appropriate IAM policies and procedures, thus creating security deficiencies. Oftentimes, IAM takes a back seat to other business initiatives during the mad dash to get projects, applications, and systems to market. Cutting corners seem to be the norm.

Even for organizations who define some level of policies, there are often enforcement deficiencies within the applicable areas of the execution model of a program and project. These deficiencies are created in part, due to gaps in communication between the authors of policy, control implementation teams, business stakeholders, risk managers, and senior leadership.

Policies should be managed in a way that includes traceability from the board level down to the solutions chosen to enforce policy. Authorizations by top executive management within the business and IT spheres, as well as compliance, should be endorsed on a regular basis throughout the lifecycle of any IAM project based on the definition of controls, associating procedures, and guidelines.

Once the foundational policies have been approved and published, IAM controls can be mapped/defined/built to support compliance across the enterprise.

IAM Controls

The IAM spheres rely greatly on controls in the form of access controls. An access control is any hardware, software, and/or policy or procedure that controls access to various assets.

Many different security controls work together to provide access control. They support the relationship between the user, or nowadays the device (Internet of Things), and the access to the asset.

The controls identified in the policies serve as the foundation to define the capabilities to deliver value to the business. The table below provides a few examples of controls mapped to capabilities:

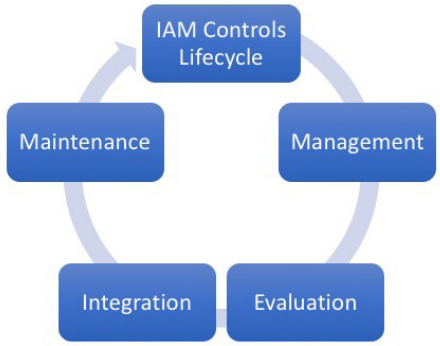
Control	Type	IAM Domain	Capability
Segregation of duties	Preventive	Identity Management / Access Governance	Define roles and rules to test for SOD conflicts
Strong Authentic-ation	Preventive/ Compensat-ing	Access Management	Stronger one and two factor auth-entication scheme
Unauthorized Access	Detective / Corrective	Identity Management	Accounts Reconcil-iation
Constrained Access	Technical	Identity and Access Management	Usage of roles and coarse / fine grained access model

Now that your controls are defined, how can you enforce them in the execution model of a program and/or project?

You need to embrace an IAM controls lifecycle to be in compliance with your policies.

The IAM controls lifecycle will support you throughout the execution of your project with the following four phases:

> Management of the controls
> Evaluation of the implemented controls
> Integration of the controls
> Maintenance in the form of improvements



The lifecycle phases are broken out as follows:

Controls Management

Controls management is part of the continuous policy management program, and the controls must be ready at the onset of a project so they can be integrated into the design stream. The activities within controls management will include:

> Plan policy changes based on the previous lifecycle, including lessons learned or postmortem of the previous project.
> Performing a risk assessment against controls including:
  > Mapping the control to an identity or access management capability to allow you to understand if the capability can be implemented within your budget and/or if the capability will be too difficult to implement - Mapping the control to an identity or access management capability to allow you to understand if the capability can be implemented within your budget and/or if the capability will be too difficult to implement
  > If it is too difficult to implement, this activity presents an opportunity to identify potential alternate controls that may denote lower complexity and lower cost to implement.
> As part of the ongoing policy management program, define the policy and/or optimize the controls.
> As need be, define the associated procedures and/or guidelines.
> Map controls to solution capabilities and place them into your personalized IAM framework.
> Define how the capability will deliver value to IT and/or business.
> Measure the values by defining metrics.

Evaluation

In this phase, you will need to evaluate or assess the controls and capabilities versus various elements as follows:

> As need be, assess capabilities for impacted assets versus data classification model.
> Assess any organizational readiness impact against complexity and culture of the organization to adopt the new capability.
> Evaluate processes, roles, responsibilities, and skills to ensure that the IAM team can operate, support, and maintain the new or changed capabilities.

Integration

This is the phase that will support you with the enforcement of the related policies and compliance, along with the identified controls now mapped as solution capabilities which will support the following activities:

> Integrate capabilities into design document.
> Create staff awareness material.

Maintenance

Once in place, this last phase will serve as input to the next iteration of the lifecycle:

> If using a service catalogue, update the IAM services within the catalogue.
> Conduct lessons learned or postmortem sessions.
> Improve the implementation and use of security measures and controls for the next iteration.

Benefits of Lifecycle

IAs policies need to be supported by executive management, the lifecycle provides an opportunity to enforce the policies and impose compliance with the controls within all aspects of various projects. More importantly, it helps bake IAM into Business as Usual processes. Finally, mapping the control to a capability allows the organization to understand potential implementation challenges and alternatives to reducing complexity or costs:

> Along with a solid governance structure, the controls will support the required management oversight to avoid slippage, common to many projects.

> Improve alignment by ensuring that every solution is designed and implemented consistent to a predefined set of policies and controls resulting in economies of scale in the longer term.

Takeaways

> Seize the opportunity to establish a solid policy framework to support your IAM program to obtain executive management team sponsorship.

> Perform the prescribed risk assessment to ensure you are performing within your budget and that you can attain your benefits by implementing pragmatic capabilities to reasonably mitigate risks.

> Map the controls to capabilities to help support your business case and to further justify the resources (budgets and time) to move forward.

> Adhering to compliance of controls throughout the execution model of a project will help allow your IAM governance structure to improve its management visibility and oversight.

> Finally, compliance of controls will support the realization of a strategic and prioritized roadmap.

About Dan Legault

Dan is a dynamic cybersecurity lead and trusted adviser, CISSP certified, who uniquely combines over 32 years of information technology experience with 22 years of cybersecurity experience. He is an expert in all areas of identity and access management and enterprise security including complex implementations, corporate security strategy, governance, enterprise risks, frameworks, and methodologies.

online business systems

Contact:
Online Business Systems
204.982.0200
rsp@obsglobal.com

About Online Business Systems

Founded in 1986, Online Business Systems is an information technology and business consultancy. We help enterprise customers enhance their competitive advantage by designing improved business processes enabled with robust and secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart. Today we have nearly 300 business and technical consultants throughout Canada and the US.