Chapter 11: Identity and Access Management Worksheet

This Help Desk improvement checklist worksheet is intended to be used in conjunction with the related chapter in the Help Desk Management Book by Wayne Schlicht.

Identity and Access Management

The identity and access management process governs the management of user identities and user access to resources within an organization. A Help Desk plays a big role in the identity and access management process. Help Desk agent's job duties include managing user identities, resetting passwords, and provisioning access to resources.

For this identity and access management worksheet, I am recommending implementing the following projects.

Step 1 – Define your Identity and Access Management process

Do you have a formally approved and documented identity and access management process? If you do, great. Well done.

If you do not, then you will need to start somewhere and document your current processes.

1. The best way to start is to perform a work in motion. Have an auditor monitor your team to identify all the identity and access management processes they do. This includes identifying the processes step by step. The processes should be documented by creating specific operational procedures.
2. Once documented, the procedures should be reviewed by security experts. The security experts will determine if there are security concerns for any of the newly documented procedures.
3. The procedures must be updated with any recommendations or requirements provided by the security experts.

Step 2 – Setup Identity and access management training

Once you have your identity and access management processes defined and documented into procedures, staff will need to be trained. It should be mandatory that your Help Desk staff receive training on security, identity, and access management policies and procedures. Security training for all Help Desk agents is an important factor in implementing a successful identity and access management program. The Help Desk agent should have training on how to recognize, document, and escalate security-related incidents.

Step 3 – Ensure User Identification Validation

When a user calls the Help Desk, it is important to ensure the caller's identity before resetting a password or performing any account maintenance. In the past, establishing user identity was performed by asking the user something they know, such as prearranged challenge questions. Establishing a user’s identity using challenge questions is no longer recommended. Compromised user accounts are one of the primary culprits in some major data breaches. Today and beyond, user identity should be established using multi-factors. These should be based on something they have (token, phone code, or security app) or something they are, such as a fingerprint or face scan. The most critical part is to ensure a process to validate the caller's identity is in place, approved, and used. Engage 3rd party vendors to provide a demonstration of their identification validation applications.

Step 4 - Implement a Self-Service Password Management Process

One of the highest call volume and cost drivers is password-related calls. Self-service password reset tools will give customers the ability to unlock, reset, and change passwords without calling the Help Desk. Self-service password reset tools can significantly reduce costs. To implement a self-service password management system, follow these steps.

1. **Gather the password management data.** The data needed include call and ticket data. We will need to know the volume of calls received and the number of tickets created. We will need to know the average duration of the calls and the cost per call. Other data may be needed. The goal of this step is to determine how much time and money your Help Desk is spending on password management.
2. **Research the current top password management systems available.** I recommend going to Gartner or Forrester to obtain a list of recommended password management systems. Reach out to multiple password management companies to set up demonstrations of their application. For more specific password management system information, please refer to this book’s companion website, BuildaHelpDesk.com.
3. **Create a finalist list.** Setup three password management vendors to provide a demonstration and a quote for their system.
4. **Select and implement the self-service password management system.** Once implemented, you should find a reduction in call flows to the Help Desk. This should improve metrics and allow you to adjust staffing levels to save money.

Step 5 – Implement Role-Based Access Control

Does your company use defined role-based access controls to permit users access only to what they absolutely need to perform their job functions? Employees must only be allowed access to resources necessary to perform their job duties. Onboarding new users is a process that occurs repeatedly. Many Help Desks expend a lot of energy trying to set up accounts ad hoc. Having an automated onboarding process can make the process smooth and manageable. Below is a highlevel list of steps needed to be completed to implement role-based access control at your company.

Step to implement Role Base Access Control (RBAC)

1. **Define the IT services you provide to your customers.** Examples of these IT services are email, applications, and file shares.
2. **Determine the roles needed for each of the IT services.** For each of the IT services, you may have different roles identified, such as an administrator, general user, and power user.
3. **Create the security groups for the IT services roles.** Access is provided by security groups. Each specific role needs to have a security group defined. Once the role is defined, permissions and security groups are assigned to that role based on the minimum access needed for someone in that role.
4. **Create business group roles.** Business group roles are set up to define specific roles in a company, such as financial analyst or human resources generalist. Then each of these roles will have whatever specific IT services roles are needed for the group to perform their job.

Implement a process to onboard, offboard, and modify the user provisioning and access process. Defining how users are placed into business roles and security groups to receive access to IT services is very important. I recommend having a workflow of resource manager approval, approvals from a user’s manager, and an auditable process trail. An automated onboarding process is usually driven by a workflow engine in the ticketing application or part of a security account management application. The hiring manager normally kicks off the process by completing a request form for their new hire. Selections are made in the form of the access the new user will need. Once submitted, the workflow engine will create tasks in the ticketing application for work teams.