**Access Management Application Specification**

**Typical User Case and Value Proposition**

All assets in medium to large size organizations are typically secured with some type of controlled access to ensure that the organization is able to maintain the confidentiality of its information. Employees of these organizations require the right level of access to execute their jobs effectively. This access needs to be tracked and managed through an employees ten-year and the assets life-cycle.

Access is added for new employees and new projects. Access is upgraded for promotions and downgraded for disciplinary action. And finally access removed when the employee moves on from the company altogether.

Similarly, assets are added for new services and products. Access for these assets is assessed based on risk and removed when the asset is retired or returned after use.

The typical way IT Industry has solved this problem is to attempt to provision the access in a single-sign-on type of tool. Invariably however, single-sign-on is a misnomer as compatibility is not perfect with all applications services and asset types. With access being managed where it is provisioned, sometimes in dozens of places, access management is still decentralized and therefore there is no way to immediately determine the status of a particular user at anytime. The organization must query each asset for each user manually – with no real way of knowing what the “correct” access should be for that asset. Most tools and thus most organizations do not have a way of knowing and documenting the correct access for assets. Each asset must be inventoried and access managed accordingly. Thus they cannot claim they truly manage access at all. They merely have password management systems.

Lets assume that their tool does in fact accomplish single sign-on:

* What about physical assets requiring old school keys or key cards that are assigned?
* What about software licenses that are assigned but aren’t being used?
* What about laptops that are assigned? How does the organization track the access to physical assets?

It seems if the asset isn’t a simple username and password its out of the control of the single sign-on.

* What about when a user leaves the company?
* What about when a user temporarily joins a project or goes on leave?
* What about approvals for access being granted or removed?

Again, it seems if the user isn’t a simple static employee and has changing access control requirements they are out of the control of the single sign-on.

The missing link is a complimentary system (to the single sign-on controls) to assign, approve and match users access given with assets access required. An exhaustive mapping of what the controls should be. Automation of this system with existing tools is key to ensure records are kept up to date and the maintenance of the system is easy to manage and the data within is up-to-date and trustworthy.

Identity-As-A-Service (IDaaS), Single sign-on (SSO) Identity and access management (IAM) are not Access Management Tools. They are Access Control Tools. They manage how the access IS not what it SHOULD to be. For example - You cannot look at OKTA, and have any confidence it set-up correctly. All you know is that the users have secure access defined at the current moment. It doesn’t tell you if assets or users are missing. It doesn’t tell you if users have too much access or even if they have left the company and still have access. It doesn’t tell you if users can access the assets physically and simply walk off with them.

**The role of this product is to complement the existing Identity Control Tools with a holistic corporate Access Management application layer.**

**Critical Success Factors for Access Management include:**

* The ability to verify the identity of a user (that the person is who they say they are)
* The ability to verify the identity of the approving person or body
* The ability to verify that a user qualifies for access to a specific service
* The ability to link multiple access rights to an individual user
* The ability to determine the status of the user at any time (e.g. to determine whether they are still employees of the organization when they log on to a system)
* The ability to manage changes to a user’s access requirements
* The ability to restrict access rights to unauthorized users (e.g. provisioning and single sign-on)
* A database of all users and the rights that they have been granted.

System must be secure!

* System planning for multiple firewalled installations is critical.

System must be smart.

* AI will be used to scan for changes in users and assets.
* AI will be used to ‘red flag’ issues.
* AI will be used to notify admins and managers when tasks are coming due, due, and over due.
  + Smart emails will be used to simplify work flow. Ie approvals within the Inbox.
* AI will be used to suggest audits.
* AI will be used to determine complex interdependencies between Users, Roles, Groups, and Assets.

Users need to be able to view and attach documents to their profiles.

Managers need to be able to approve Users and add Assets within their scope.

Admins need to be able to manage Access Control with less work than not using the system.

**Typical Inputs and Outputs**

A standard access request is typically generated by the Human Resource system. This is generally done whenever a person is hired, promoted, transferred or when they leave the company.

* Job changes. In this case the user will possibly need access to different or additional services.
* Promotions or demotions. The user will probably use the same set of services, but will need access to different levels of functionality or data.
* Transfers. In this situation, the user may need access to exactly the same set of services, but in a different region with different working practices and different sets of data.
* Resignation or death. Access needs to be completely removed to prevent the username being used as a security loophole.
* Retirement. In many organizations, an employee who retires may still have access to a limited set of services, including benefits systems or systems that allow them to purchase company products at a reduced rate.
* Disciplinary action and temporary leave. In some cases the organization will require a temporary restriction to prevent the user from accessing some or all of the services that they would normally have access to. There should be a feature in the process and tools to do this, rather than having to delete and reinstate the user’s access rights.
* Dismissals. Where an employee or contractor is dismissed, or where legal action is taken against a customer (for example for defaulting on payment for products purchased on the Internet), access should be revoked immediately. In addition, Access Management, working together with Information Security Management, should take active measures to prevent and detect malicious action against the organization from that user.

Another standard access request is typically generated from a Request for Change system. This is generally done whenever a product, process or project is added, revised or depreciated/completed.

* Product/service changes. This is most frequently used for large-scale service introductions or upgrades where the rights of a significant number of users need to be updated as part of the product or service.
* Process changes. In some cases process steps requiring access control can be added or removed from the system. A review and audit of the change may be required to ensure the change is implemented effectively and operations continue as normal.
* Project changes. Many organizations and indeed IT departments manage large standard tasks or assignments as projects. Projects can include everything from on boarding a new customer to integrating a new tool to subcontracting a service to a new vendor. Projects may involve managing access controls for groups of users and assets.
* Physical asset changes. Most IT processionals are focused on virtual technology. Key cards, key fobs, punch codes, filing cabinet keys, door keys, safe codes, security company disarm codes, etc are easily forgotten and availability and confidentiality for these physical assets can become at risk.

A Service Request submitted or Incident Management system deficiency.

* A Service Request. This is usually initiated through the Service Desk, for lost/forgotten passwords or other user access issues on an exception basis. The goal of access management is to identify the user and confirm the request is within the user’s rights.
* Incident Ticket. This is usually directly from an Incident Management system and executed with the relevant Technical or Application Management teams. Any deficiency identified with the access control system should be investigated and corrected with the highest priority.
* Audit and regulatory compliance. This is usually initiated through the Service Desk on a regularly scheduled basis to ensure compliance to relevant regulatory, customer and standard requirements. A statistically significant sample of users and assets are selected for review and a record of compliance is kept. Any noncompliance must be escalated to the Incident Management System with top priority.

**Phased Development**

**2 – Create the commercial platform**

1. Commercial website
2. E-commerce
3. Free trial
   1. Create environment
4. Ops Website
   1. Sign on
   2. Segregation of client environments
   3. Database architecture, encrypted
   4. Environments firewalled from each other

**1 – Create the basic structure of the repositories.**

1. Approvers
2. Users
3. Assets
4. Roles
5. Groups
6. Ticket System
7. Audit System
8. System Admin Set-up
9. AI Engine Set-up



**User Story 1 – Basic Manger Workflow**

1. Daniel onboards a new employee.
2. Daniel reviews the Role –
   1. A new Role needed to be created this new hire.
   2. Assets and access are assigned to the Role
3. Daniel creates the User and completes the profile as required. User Status is set to ”New”
   1. Assigns the Name.
   2. Assigns the Role.
   3. Attaches the documents.
   4. Assigns Laptop Asset.
4. Daniel sends the User for Approval – Email shows Access Config and missing info in highlighted.
   1. Ticket is created in Ticket System and set to ”Sent for Approval”
   2. User Status is set to ” Sent for Approval” and locked for editing.
5. Daniel approves the Access. Ticket Status is set to ”Approved” User Status is set to ”Approved”
6. Daniel assigns Access in the appropriate systems as required.
7. Daniel closes the Ticket. Ticket Status is set to ”Access Granted”

**User Story 2 – New User Workflow**

1. HR onboards a new employee.
2. HR sends the Ticket Module an email indicating new hire Name and Role.
   1. Attached NDA and Contract.
   2. This user will need to be issued a laptop.
3. Ticket appears on the Dashboard as ‘New’.
4. IT admin reviews the Role – A new Role may need to be created with HR/Managers for this new hire.
5. IT admin creates the User and completes the profile as indicated in the Ticket.
   1. Assigns the Name linked to AD
   2. Assigns the Role.
   3. Attaches the documents.
   4. Assigns Laptop Asset.
6. IT sends the User for Approval (Approver is typically the user’s Manager) – Email shows Access Config and missing info in highlighted.
   1. Ticket Status is set to ”Sent for Approval”
   2. User Status is set to ” Sent for Approval” and locked for editing.
7. Approver reviews the User Access.
8. Approver rejects the Access. – Indicates a missing Group for a project. - Email response is added to the Ticket. Ticket Status is set to ”Rejected” User Status is set to ”Approval”
9. IT actions the ticket and resends the User for Approval – Email shows Access Config. Ticket Status is set to ”Sent for Approval”
10. Manager approves the Access.
    1. Ticket Status is set to ”Approved”
    2. User Status is set to ”Approved”
11. IT grants the Access in the appropriate systems as required.
12. Laptop given to user
13. IT closes the Ticket. Ticket Status is set to ”Access Granted”

**User Story 3 – New Asset Workflow**

1. Nagesh creates a new internal commercial website for a new app.
   1. Only Managers and Admins can create new assets
   2. Manager Logs into the system (limited options) click on <New Asset> form homepage.
2. Nagesh creates a new Asset in the system.
   1. Assigns the Asset Description
   2. Assigns Date Asset First Active:
   3. Enters Asset Location
   4. Assigns Asset Owner: <Dropdown list>
   5. Assigns Risk Ranking: <Dropdown list> Low
   6. Enters Asset type: <Dropdown list> Website
   7. Attaches Asset Info: such as the URL and Admin Login information.
3. Nagesh assigns the Asset to an existing Role ‘website administration’
4. On save and exit: Workflow
   1. System queries which users are effected by the change - that need to be granted access
   2. User status is set to “Modified” for users affected.
   3. Ticket is created for each user affected.
5. System sends the User for Approval (Approver is typically the user’s Manager) – Email shows Access Config and missing info in highlighted.
   1. Ticket Status is set to ”Sent for Approval”
   2. User Status is set to ” Sent for Approval” and locked for editing.
6. Approver reviews the User Access.
7. Approver approves the Access.
   1. Ticket Status is set to ”Approved”
   2. User Status is set to ”Approved”
8. Dashboard shows ticket is approved and implementation is required.
   1. Email notifications are sent:
      1. Notification of approval / action required,
      2. Coming due
      3. Due
      4. Over due
9. IT grants the Access for the user to access the website as required.
10. IT closes the Ticket. Ticket Status is set to ”Access Granted”

Ticket system list of action items.

AI Dashboard groups together “tickets” by User or Asset.

* Approval ticket
  + Requested
  + Approved
  + Rejected
  + Closed
* Standard workflows (that don’t require adding users or groups or assets)
  + Add access ticket
  + Remove access ticket

**User Story 2 – New Asset Workflow**

1. Slawek onboards a new customer.
   1. The project is to update an existing website
2. Slawek creates a new Asset in the system.
   1. Assigns the Asset Description:
   2. Assigns Date Asset First Active:
   3. Asset Location
   4. Asset Owner: <Dropdown list>
   5. Risk Ranking: <Dropdown list> (High/Medium/Low)
   6. Asset type: (Website, Tool, Certificate, Software, Equipment, Location) <Dropdown list>
   7. Attach Asset Info:

**Access Management Technical Elements**

Application Layout



Application Description

|  |  |
| --- | --- |
| **Dashboard - Main Menu OPTIONS** |  |
| Log-in and system access Module | Systems users are set-up in the System Admin Module.  Admin – Read / Write / Delete Access to all modules in the system. Escalation emails are sent to Admins. The Admin(s) run the system, reviewing the dashboard and ensuring tickets are actioned and closed.  Managers / Approvers - Read / Write / Delete Access to Users, Assets, Roles and Groups. Managers are often approvers. Approval emails are sent to Approvers.  Managers / Approvers – Read access to the homepage / Dashboard for reporting and monitoring.  Users – Read Access to User profile. Users don’t need to be added to the system separately form their User profile for read access. Dynamic Email is sent to the user with the data rather than authenticate them on the system?  Auditors – Read / Write / Delete access to the Audit module. Auditors get audit notifications and complete audits trails in the Audit module. |
| Ticketing Module | Tickets are used to track workflow.  AI Workflow can create tickets  Admins and Managers can create tickets. |
| Auditing Module | Audit schedule and audit records are stored here. Access to System Logs. |
| System Admin Module | Global System Settings (Logo, connector tool settings ie SSO / skin colours, etc) |
| AI System Admin Module | AI Workflows are modular and enabled / disabled here. A detailed description of each and settings are listed/configured here.  All approval and notification emails are AI workflows  All dashboard charts and graphs are AI. workflows.  All dashboard red flags are AI Workflows  All scans are AI workflows  All Weekly, Monthly health status emails are AI workflows |

Dashboard Menu

|  |  |
| --- | --- |
| **Dashboard - Main Menu OPTIONS** |  |
| Add / View Approvers | Link to Approver Page   * Admins |
| Add / View Users | Link to Users Page   * Admins, Managers, Approvers * Users auto directed to Read User Page |
| Add / View Assets | Link to Assets Page   * Admins, Managers |
| Add / View Roles | Link to Roles Page   * Admins, Managers |
| Add / View Groups | Link to Groups Page   * Admins, Managers |
| Ticket System | Link to Ticket Module   * Admins, Managers |
| Audit System | Link to Audit Module   * Admins, Auditors |
| System Admin Set-up | Link to System Admin Page   * Admins |
| AI Engine Set-up | Link to AI Engine Page   * Admins |

**Dashboard Layout**



|  |  |
| --- | --- |
| **Dashboard – Page** |  |
| Main Menu Options | Element is on every page |
| General Alerts and System Status Summary | $User\_Name != AD |
| AI User Red flags Summary | $User\_Link\_Roles = “”  $User\_Link\_Groups = “”  $User\_Link Approver = “”  $User\_NDA\_Expiry < @Today  $User\_BGC\_Expiry\_< @Today  $User\_Cert\_Expiry\_Date < @Today  $User\_Name $Role\_NDA\_Required = TRUE & $Role\_NDA = “”  $Role\_BGC\_Required = TRUE  $Role\_Cert\_Required = TRUE  $User\_Name $Group\_NDA\_Required = TRUE  $User\_Name $Group\_BGC\_Required = TRUE  $User\_Name $Group\_Cert\_Required = TRUE  $User\_Name $Role\_NDA\_Required = TRUE  $User\_Name $Role\_BGC\_Required = TRUE  $User\_Name $Role\_Cert\_Required = TRUE  $User\_Expiration\_Date < @Today  $User\_Approval\_Status != “Approved” $User\_Link\_Roles = “” & $User\_Link\_Groups = “” & $User\_Link\_Assets = ”” |
| AI Equipment Red flags Summary | $Asset\_Expiration\_Date < 1@Today |
| Due (Overdue) Approvals Summary | $User\_Approval\_Status = “Over Due” |
| Due (Overdue) Tickets Summary | $Ticket\_Status = “Over Due” |
| Due (Overdue) Audit Summary | $Audit\_Status = “Over Due” |

**Approver Layout**



|  |  |
| --- | --- |
| **Add / View Approver - Page** |  |
| Add Approver | List Approvers: |
| Edit Approver | Approver | Title | Roles Assigned |
| Delete Approver (Archive) |  |

|  |  |
| --- | --- |
| **Add / View Approver - Form** |  |
| Approver Name: <Dropdown from AD>  Approver Title: <Auto fill from AD – Editable> | $Approver\_Name (Name)  $Approver\_Title (Text) |
| Approver Roles: <Dropdown from Roles> | $Approver\_Link\_Roles (Text) |
|  |  |
| Hidden – System Generated | $Approver\_ID |
|  | Data collected to facilitate AI. |

User Layout



|  |  |
| --- | --- |
| **Add / View User - Page** |  |
| Add User |  |
| Edit User |  |
| Delete User (Archive) |  |
| Send for Approval |  |

|  |  |
| --- | --- |
| **Add / View User - Form** |  |
| User Name:  User Title: <Auto fill from AD – Editable>  User Unique ID Number:  Date User First Active:  User Type: <Dropdown: Employee, Subcontractor, Customer, Supplier, Other> | $User\_Name (Name)  $User\_Title (Text)  $User\_ID\_Number (Number)  $User\_Initiation\_Date (Date)  $User\_Type (Text) |
| Attach Profile Picture:  Attach ID Picture:  Attach Contracts and NDA Document(s):  Expiry / Review Date:  Attach Background Check Document(s):  Expiry / Review Date:  Attach Applicable Cert Document(s):  Expiry / Review Date: | $User\_Attach\_Pic (RichText)  $User\_Attach\_ID (RichText)  $User\_Attach\_NDA (RichText)  $User\_NDA\_Expiry\_(Date)  $User\_Attach\_BGC (RichText)  $User\_BGC\_Expiry\_(Date)  $User\_Attach\_Cert (RichText)  $User\_Cert\_Expiry\_Date (Date) |
| Date User Ends Activity / Review: | $User\_Expiration\_Date (Date) |
| Approver Name: <Dropdown from Approvers>  Approval Date:  Approval Status: Default = “Not Approved” | #Approver\_ID (Number)  $User\_Link Approver  $User\_Approval\_Date |
| Add Role:  Add Group:  Add Asset: | $User\_Link\_Roles  $User\_Link\_Groups  $User\_Link\_Assets |
| Display Workflow | $User\_Approval\_Status(Text) |
| Button Workflow | Save / Approve / Reject / Send for Approval |

Asset Layout



|  |  |
| --- | --- |
| **Add / View Asset - Page** |  |
| Add Asset | List Asset: |
| Edit Asset | Asset | Asset Description | Location | Owner |
| Delete Asset |  |

|  |  |
| --- | --- |
| **Add / View Asset - Form** |  |
| Asset Description:  Asset Unique Identification Number:  Date Asset First Active:  Asset Location  Asset Owner: <Dropdown list>  Risk Ranking: <Dropdown list> (High/Medium/Low)  Asset type: (Website, Tool, Certificate, Software, Equipment, Location) <Dropdown list>  Attach Asset Info: | $Asset\_Name (Name)  $Asset\_ID\_Number (Number)  $Asset\_Initiation\_Date (Date)  $Asset\_Location (Name)  $Asset\_Link\_Owner (Name)  $Asset\_Risk (Text)  $Asset\_Type (Text)  $Asset\_Info (RichText) |
| Date Asset Ends Activity / Review: | $Asset\_Expiration\_Date (Date) |
|  |  |

Roles Layout



|  |  |
| --- | --- |
| **Add / View Asset - Page** |  |
| Add Roles | List Roles |
| Edit Roles | Role | Role Description |
| Delete Roles |  |

|  |  |
| --- | --- |
| **Add / View Role - Form** |  |
| Role Name: | $Role\_Name (Name) |
| Role Description: | $Role\_Description (Text) |
| Attach Job Description: | $Role\_Attach\_Description (RichText) |
| NDA required ?  Background check required?  Certifications required? | $Role\_NDA\_Required (Boolean)  $Role\_BGC\_Required (Boolean)  $Role\_Cert\_Required (Boolean) |
| LINK assets to the Asset: <Dropdown from Assets> | $Role\_Link\_Assets |
| LINK assets to the Group: <Dropdown from Groups> | $Role\_Link\_Groups |

|  |  |  |
| --- | --- | --- |
| **Each Linked Asset** | **Default Access Levels** | **Special Access** |
| Asset Name | Read | Write | Full | Admin | <Editable> |
|  |  |  |
|  |  |  |

Groups Layout



|  |  |
| --- | --- |
| **Add / View Group - Form** |  |
| Group Name: | $Group\_Name (Name) |
| Group Description: | $Group\_Description (Text) |
| Attach Group Description: | $Group\_Attach\_Description (RichText) |
| NDA required ?  Background check required?  Certifications required? | $Group\_NDA\_Required (Boolean)  $Group\_BGC\_Required (Boolean)  $Group\_Cert\_Required (Boolean) |
| Date Group Ends Activity / Review: | $Group\_Expiration\_Date (Date) |
| LINK assets to the Asset: <Dropdown from Assets> | $Group\_Link\_Assets |
| LINK assets to the Role: <Dropdown from Roles> | $Group\_Link\_Roles |

|  |  |  |
| --- | --- | --- |
| **Each Linked Asset** | **Default Access Levels** | **Special Access** |
| Asset Name | Read | Write | Full | Admin | <Editable> |
|  |  |  |
|  |  |  |