Serving Government Modernization Project

Functional Requirements Document

March 2024

Table of Contents

[Review and Approval 3](#_Toc172805986)

[Introduction and Background 4](#_Toc172805987)

[Purpose 4](#_Toc172805988)

[Terms 4](#_Toc172805989)

[Portal Access Management 6](#_Toc172805990)

[Assumptions 6](#_Toc172805991)

[User Authorization (UA) 6](#_Toc172805992)

[Authentication & Authorization (AA) 7](#_Toc172805993)

[User Profile (UP) 9](#_Toc172805994)

[Organization Dashboard (OP) 11](#_Toc172805995)

[Targeted Communications 11](#_Toc172805996)

[Business Requests (BR) 12](#_Toc172805997)

[Organization Reporting (OR) 13](#_Toc172805998)

[Appendix A: User authentication & Authorization Process 16](#_Toc172805999)

[Appendix B: News & Communique Types 17](#_Toc172806000)

[Appendix C: Security Roles Requirements 18](#_Toc172806001)

# Review and Approval

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reviewer | Division | Branch | Approved By  (on behalf of Reviewer) | Date |
| Di Gioacchino Aldo | CE Portfolio Operations | Operations and Client Services Branch (OCSB) | Di Gioacchino Aldo | Feb 27, 2024 |
| Joseph-Carl Théodat | Client Executive (CE) | Operations and Client Services Branch (OCSB) | Joseph-Carl Théodat |  |
| Marc Gagnon | Client Executive (CE) | Operations and Client Services Branch (OCSB) | Marc Gagnon | Mar 08,  2024 |
| Julie McIntosh | Client Executive (SDM) | Client Service Delivery and Management Branches (CSDMB) | Julie McIntosh |  |
| Elizabeth Caswell | Service Delivery Management (SDM) | Client Service Delivery and Management Branches (CSDMB) |
| Jaspaul Parmar | Client Executive (CE) | Operations and Client Services Branch (OCSB) | Jaspaul Parmar | Feb 23, 2024 |
| Adrienne Turgeon | Service Portfolio Management | Operations and Client Services Branch (OCSB) | Farah Shakil | Feb 22, 2024 |
| Farah Shakil | Service Portfolio Management | Operations and Client Services Branch (OCSB) |
| Akram Suleman | Service Portfolio Management | Operations and Client Services Branch (OCSB) |
| Jean-Rock Drouin | Telecommunications Services | Digital Services Branch (DSB) | Jean-Rock Drouin | Feb 23, 2024 |
| Louis Varin | Telecommunications Services | Digital Services Branch (DSB) |
| Gaby Mai | Enterprise Information Services (EIS) | Enterprise IT Procurement and Corporate Services Branch (EITPB) | Colin Paveling | Feb 23, 2024 |
| Colin Paveling | Enterprise Information Services (EIS) | Enterprise IT Procurement and Corporate Services Branch (EITPB) |
| Michael Gosselin | SEB and Outreach Initiatives | Strategy and Engagement Branch (SEB) | Marianne Bergeron | Feb 20, 2024 |
| Seamus O'Brien | SEB and Outreach Initiatives | Strategy and Engagement Branch (SEB) |
| Marie-Eve Samson | SEB and Outreach Initiatives | Strategy and Engagement Branch (SEB) | Marie-Eve Samson | Feb 29, 2024 |
| Mike Spivock | Enterprise Transformation | Strategy and Engagement Branch (SEB) | Mike Spivock | Feb 26, 2024 |
| France Gravelle | SEB and Outreach Initiatives | Strategy and Engagement Branch (SEB) | France Gravelle | Feb 29, 2024 |

# Introduction and Background

Serving Government (https://service.ssc-spc.gc.ca) is a Government of Canada Extranet web platform used to support SSC’s Partners and clients which includes over 280,000 users. The web platform is used exclusively by SSC partners and clients to learn about SSC Services including email, networks, data centers, end-user IT and workplace technology devices.

SSC also launched the Serving Government Modernization project which began in October. The guiding vision for the future state Serving Government is the addition of an authenticated portal. The portal aims to allow clients a seamless experience for Organization specific content. In addition, the modernized portal will speak with one SSC voice, providing a single source of truth for SSC services. Stream one included transforming the site into a powerful information site, building all the features associated with the anonymous section of the site. Stream two, for which this document applies, builds the foundation for the personalization and all reporting functionality.

# Purpose

This document acts as the central repository for capturing the functional requirements for Stream Two of the modernized Serving Government (SG) portal minimal viable product (MVP), planned for release in fall 2024. The MVP scope will introduce a personalized section to the existing site, allowing designated personnel from a small number of partner organizations access to information and services relevant to their organization. In future releases, the portal will be made available for partners and clients.

These requirements were derived from consultations with the client executive team (CE team) during Phase 3 of the initiative and subsequent validation exercise. The final report for the client engagement may be found [here](https://gcdocs.gc.ca/ssc-spc/llisapi.dll/link/137820231).

# Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Portal | Refers to the authenticated section of the site. Where authenticated users can access to their organization dashboard. |
| Organization | Refers to any Government of Canada (GC) entity that has been given access to the authenticated section of the SG site. For a full list of organizations, please refer to this [link](https://service.ssc-spc.gc.ca/en/page/partner-and-client-mandatory-and-optional-services). |
| Onboarded organization | Refers to an organization who is on the target list of organizations for the portal and where the portal is ready to serve the users of this organization. |
| Candidate user | Refers to a person from an organization that has NOT yet been authorized to access the portal. |
| Authorized user | Refers to a person that has been added to the list of authorized users in the portal, which includes associating the user with an organization. |
| Authenticated user | Refers to an authorized user that has successfully logged into the portal. |
| Anonymous component of the site | A Serving Government feature available to every user without the need to authenticate themselves. |
| Authenticated component of the site | A Serving Government feature that is available to certain users and requires authentication prior to access. |

# Portal Access Management

## Assumptions

Access to the SG portal authenticated component of the site will be restricted to a small group of users within each organization. Organizations are expected to contact their service delivery manager (SDM) to request access. A business process will need to be developed, documented and published internally and externally to outline the SG portal access request review, approval and implementation process.

## User Authorization (UA)

|  |  |
| --- | --- |
| **BR#** | **Description** |
| UA1 | Portal access is restricted to those that have been approved by their CE or SDM (see Assumptions) and controlled within the application |
| UA2 | Authenticated user access is approved using the process as described in the [Assumptions](#_Assumptions) above. This is a component of the authorized user management functionality required (UE3 below). |
| UA3 | The portal will manage authorized users with an organization user management role.  Refer to “organization user management role” in Appendix C: Security Roles Requirements.   The following is a list of user management operations that will be supported:   1. Ability to add a new user to the list of authorized users. A user must be associated with an organization. Once a user has been added to the list of authorized users for that organization, they are considered authorized. 2. Ability to remove a user from the list of authorized users. Once a user is removed from the list of authorized users for that organization, they are no longer considered authorized.   Note that the operations above will be done manually either:   1. In the portal “back-end”   OR   * Through functionality (forms and the like) that would be developed to provide a simpler interface to perform these activities by a user with user management role. |
| UA4 | Once a candidate user is authorized, the user will be added to the organizations authorized user list which gives them:   1. Access to login to the portal 2. Access to their organizational dashboard containing all information, features and reports in the portal pertaining to their organization   Refer to “Authenticated users” role in [Appendix C: Security Roles Requirements](#_Appendix_C:_Security). |
| UA5 | The application has controls in place to ensure that users are NOT linked to the wrong organization. |
| UA6 | The application will need to store a list of organizations and include the following fields:   1. Organization acronym 2. Organization type with the following values:    1. Partner    2. Client 3. Organization name 4. Whether the organization has been **onboarded** to the portal or not 5. Other fields that the overall solution may require/use   The broad readiness criteria for an onboarded organization involves confirming that the application has the information and the accuracy to properly serve that organization. The exact criteria will need to be established during the application design and development. |
| UA7 | Organization Administrators will be able to consult the list of organizations and set an organization as onboarded. |
| UA8 | Initial load and changes to the organization information in UE6 will be done manually by individuals with organization administrator role.  Refer to “organization administrator role” in [Appendix C: Security Roles Requirements](#_Appendix_C:_Security). |
| UA9 | When an organization is onboarded (refer to UA6), it indicates that the authorized users against that organization may be able to access the portal. |

## Authentication & Authorization (AA)

Refer to [Appendix A: User authentication & Authorization Process](#_Appendix_A:_User) for a process flow articulating the proposed authentication and authorization process.

|  |  |
| --- | --- |
| **BR#** | **Description** |
| AA1 | The portal supports authenticating the user using single sign-on by leveraging the users’ organization Azure AD tenant (i.e. organization email and password). Organizations that do not have an Azure AD tenant will not be able to access the authenticated or anonymous section of the site. |
| AA2 | The portal restricts access to onboarded organizations only (refer to UE6). If a user from an organization that has not been onboarded tries to login, the portal:   1. Indicate to the user that they are NOT authorized to access the Serving Government Portal yet and to refer to their SSC service delivery manager (SDM) for more details (exact message will be drafted by the communications team). 2. Redirect the user back to the home page |
| AA3 | The portal should restrict access to authorized users only. If a user that has not been authorized tries to login, the portal should:   1. Indicate to the user that they are NOT authorized to access the Serving Government Portal yet and to refer to their SSC service delivery manager (SDM) for more details (exact message will be drafted by the communications team). 2. Redirect the user back to the home page |
| AA4 | The portal should support multi-factor authentication (MFA) using one of the approved GC MFA methods. |
| AA5 | When a user logs in to the site, they will be directed to an Edit Information page where they will be required to populate any missing **mandatory** fields of their portal profile before being allowed to proceed. For a list of mandatory fields, refer to [UP1](#UP1) and UP2. Clicking any links such as the logo, home, etc will result in the user being left on the Edit Information page until these mandatory fields are populated and saved. |
| AA6 | The portal must create, protect and retain audit logs and event records. This is to help detect, determine the scope of, understand and recover from attacks. Logs must include sufficient information to establish what events occurred, and who or what caused them and when. At a minimum, the following events must be logged:   * Successful and failed sign in attempts (login attempts); * Sign outs (logoffs); * User, role, group and organization additions, deletions, and modifications; * Successful and failed attempts of modification to user permissions e.g. privilege elevation; and * Any other relevant security alerts and failures. |
| AA7 | Audit logs and event records must be retained in accordance with the Library and Archives Canada (LAC) and SSC standards:   * Events and logs must be retained for at least 3 months online and at least 6 months in storage; * Events and logs associated with security incidents must be retained for at least 2 years; and * Events and logs must be retained for a period of 2 years after last administrative use for information with business value in IT or security purposes. |
| AA8 | Audited events must be forwarded to an approved GC centralized security information and event management (SIEM) system. |
| AA9 | Audit logs and event records must be protected against tampering and unauthorized access. |
| AA10 | Associate users with a general role within the organization[[1]](#footnote-2). This will give all users in that organization access to the organization’s content and Organizational report. Additionally additional roles will be provided for access to additional reports. |
| AA11 | Provide access to **content editors** to add and change content for the authenticated component of the site. These content editors will be **SSC users only**. This group will be an additional content editor role with access to update information published on the portal (vs. the existing content editor group capable of publishing content and making changes to the content on the anonymous section of the site). |
| AA12 | Continue to support the ability for the communications team to edit content on the site by introducing a special role that provides the necessary level of access while restricting the ability to edit ALL content.  For more information, refer to the “communications” role under [Appendix C: Security Roles Requirements](#_Appendix_C:_Security). |
| AA13 | Support the ability for a designated team to support the SG application by having the ability to edit all content on the site.  For more information, refer to the “Editor” role under [Appendix C: Security Roles Requirements](#_Appendix_C:_Security). |
| AA14 | If an authenticated user has no activity on the SG site for 30 minutes, a dialog shall appear, displaying a warning of a 60 second grace period to extend the session or otherwise an auto logout will occur. |
| AA15 | An authenticated user, upon logging out, is redirected to the landing page and no longer has access to portions of the site that require authentication (e.g. the Primary Reports page) |

## User Profile (UP)

|  |  |
| --- | --- |
| **BR#** | **Description** |
| UP1 | The user profile will contain the following fields that are **not editable:**   * User email address from the user departmental tenant * **Full name** of the user, if available from the user departmental tenant.   These attributes will be captured and stored from the organization’s Azure AD tenant. The viability of capturing this information from the organization’s Azure AD tenant will be confirmed in the design and validation phase. |
| UP2 | The user profile will contain the following additional fields:   * **Job Title (mandatory)**, where the user will be able to select one of the following options:   1. **Supervisor**   2. **Manager**   3. **Director**   4. **Senior Director**   5. **Director General**   6. **Assistant Deputy Minister**   7. **Other** * **Role (mandatory)**, where the user will be able to select one of the following options:   1. **SSC Liaison**   2. **Chief Information Officer (CIO)**   3. **CIO Advisor**   4. **Communications Officer** * **Other (specify)**, user will be asked to specify the role   Information captured from the organization Azure tenant will be stored and/or used in the application and will not be editable, while fields that are either not in organization Azure tenant or are unreliable will be editable by the authorized user. Additional fields may be added during the design and implementation phase.  These fields will provide important insights into the roles of the users accessing the portal and thus, maybe used in the future to tailor the content to the user. |
|  |  |

# Organization Dashboard (OP)

|  |  |
| --- | --- |
| **BR#** | **Description** |
| OP1 | Page identifies user’s organization |
| OP2 | User has the ability to navigate to their profile settings. This page is titled Edit Information and contains contact and professional information. (see UP) |
| OP3 | Ability to navigate to and consult PowerBI reports belonging to the users’ organization |
| OP4 | Ability to view, filter and search communications targeted to the users’ organization |

# Targeted Communications

The anonymous site communiqué section will continue to include communiqué types that are available and sharable across all SG clients. Currently, the following are all considered communiques:

1. SSC Gateway
2. CIO communiqués

The new authenticated section of the site will host “targeted communications”, which are news and communiqués that are targeted to specific clients and are not typically shared with other organizations.

|  |  |
| --- | --- |
| **BR#** | **Description** |
| TC1 | Platform will support the ability to publish targeted communication for authenticated users which includes the following types:   * Infrastructure Change Notice (ICN) – refer to [appendix](#_Appendix_B:_News) for more information about ICN. * CIO communiqué refer to [appendix](#_Appendix_B:_News) for more information about CIO communiqué |
| TC2 | The ICN Author is responsible for creating ICNs. When creating an ICN it is required to select the organization(s) impacted. There is no limitation on the number of organizations selected. |
| TC3 | The ICN Author can save the ICN as draft and publish the ICN when it is complete. The ICN will not publish if it has not been translated as the ICN text is used to generate the email sent to the distribution list upon publishing. |
| TC4 | Ability for **Client Organization’s users** to access, filter and search ICN and CIO communiqué on their organization page. |
| TC5 | The ICN Distribution list manager team will be provided exclusive access to forms that allow them to manage the ICN distribution lists. The form will require them to select the organization and provide a list of emails to associate with this organization. The form will include a check on emails provided to ensure that these emails belong to the selected organization.  These forms will also provide the ability to update these distribution lists by adding, removing and updating emails associated with that distribution list for target organization. Organizations will **not** be able to edit their own distribution list in MVP release. |
| TC6 | The platform will email people on the distribution list for selected partner organizations (including ones that are not onboarded) when ICNs are puslished. This would include when a published ICN is edited/updated.  Members of the distribution list that are either not authorized or belong to an organization that has not been onboarded will not be able to view the ICN on the portal but will receive an email from the site containing the ICN. |
| TC7 | Events related to the creation and management of targeted communication distribution lists and/or access management will be logged for auditing. |
| TC8 | The site will need to send the emailed ICN from the following email: [servinggovernment-auservicedugouvernement@ssc-spc.gc.ca](mailto:servinggovernment-auservicedugouvernement@ssc-spc.gc.ca) |
| TC9 | When the “when” end date is stale (past current date), provide a warning message on save stating that the ICN  email was not sent to the distribution list(s) due to the stale date(s). |
| TC10 | Basic draft/live workflow to allow editing a draft state, complete translating before publishing/triggering an ICN email. |

# Business Requests (BR)

During MVP planning, the decision was made to de-scope integrating into the Business Intake Tracking System (BITS) and leverage reporting to show BR information. The evaluation for integrating into BITS will be assessed in future phases. Refer to the [Personalized Reporting section](#_Personalized_Reporting_(RP)) for information about the BR information that will be exposed in MVP.

Report Embedding (RE)

|  |  |
| --- | --- |
| **RE#** | **Description** |
| RE1 | The platform has the ability to embed PowerBI reports (see Organization Reporting). |
| RE2 | Two types of reports are supported:   * Global reports: available to all Organizations * Organization specific reports: Assigned to specific Organizations. |
| RE3 | All authenticated users of an Organization have access to all Global reports. |
| RE4 | Organization specific reports may be assigned access to specific users within that Organization. |
| RE5 | Reports can be switched between English and French. |

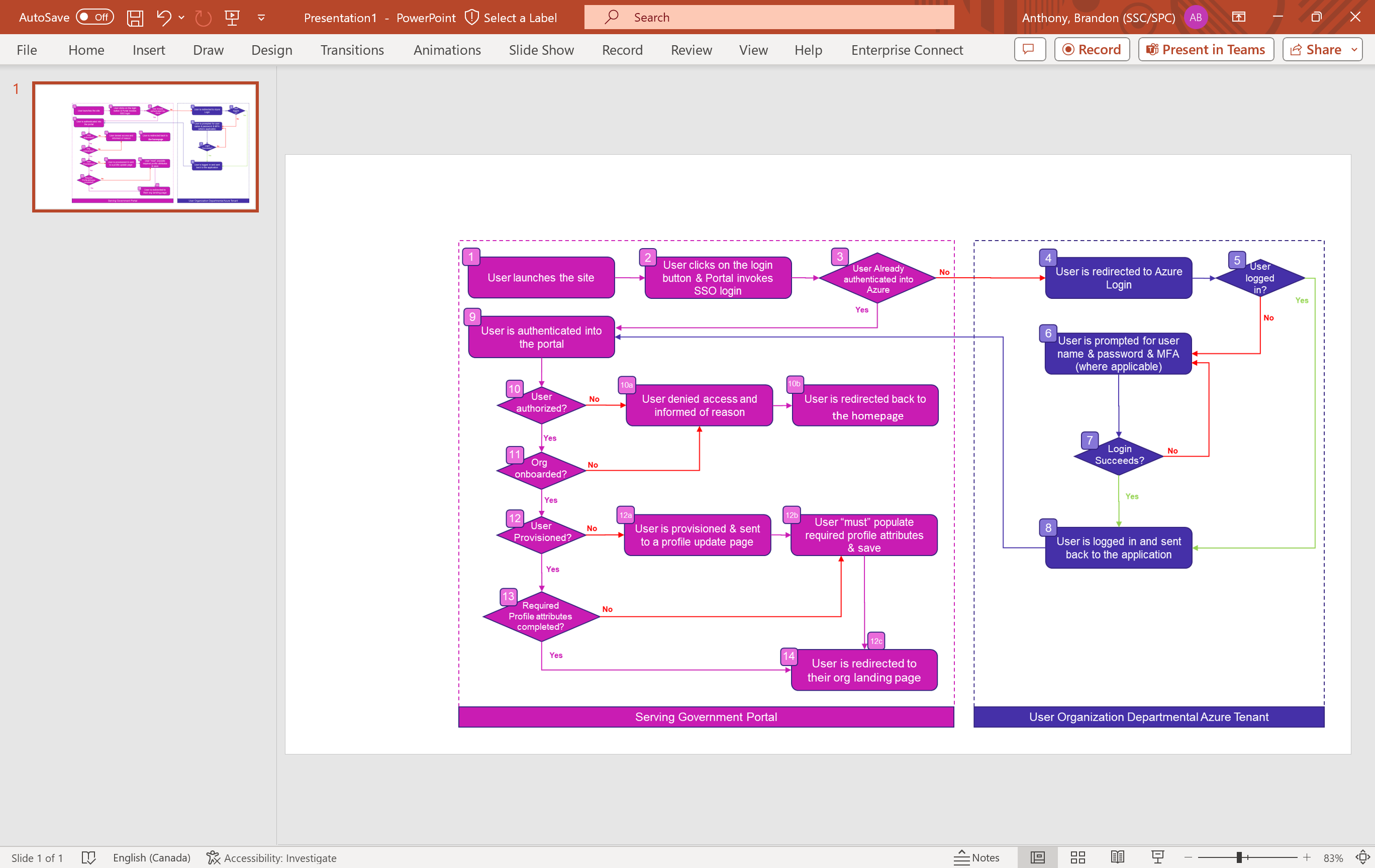
**r**

# Organization Reporting (OR)

*For reference: Detailed descriptions of the content of the reports targeted for MVP is available in the* [*MVP report list document*](https://163gc.sharepoint.com/:w:/r/sites/SGModernization/Shared%20Documents/Phase%204/Reporting/SG%20Modernization%20development%20roadmap%20-%20Report%20list.docx?d=w12b7b8e5d2b4456597c339df915605c9&csf=1&web=1&e=1FOImO)

|  |  |
| --- | --- |
| **BR#** | **Description** |
| OR1 | Reporting Dashboard. Offers an overview of the ongoing business requests, service requests, incidents, change requests and consumption metrics for the department. Acts as a gateway to the other reports.  **Sections**   * Business requests   + Count of active business requests by priority, Count of active business requests by phase, Count of active business requests by implementation flag. * Service requests   + Count of active service requests by priority, Count of closed service requests for the selected period by priority. * Change requests   + Count of active change requests by priority, Count of closed change requests for the selected period by priority. * Incidents   + Count of active incidents by priority, Count of closed incidents for the selected period by priority. * Consumption metrics   + Count of actual service consumption units, Variance of service consumption units over the selected period. |
| OR2 | Business requests report. Offers an overview and details of the department’s business requests. A variety of filters are available to drill down and explore business requests. This report presents estimated agreement cost information as well as delivery metrics (cycle time by phase, implementation time).  **Sections**   * Overview of business requests   + Count of business requests by priority of request, Count of business requests by phase, Count of active business requests by implementation flag, Count of active business requests by complexity, Count of business requests by service, Business requests SLA by service, Count of business requests over the selected period. * Business requests details   + BR number, title, requirement overview, priority lead service, supporting services, current phase, current status, days in status, submission date, days since submission, target implementation date, amount of billing, related configuration items.   + Estimated Agreement Costs Amount of estimated costs by service. * Delivery   + Average cycle time by phase, Average implementation time. |
| OR3 | Incidents report. Offers an overview and details of the department’s incidents. This report offers a higher level of details for critical and high priority incidents (cause, impact, resolution), and informs the user about which other departments were also affected by the incident impacting his own department.  **Sections**   * Overview of incidents   + Count of active incidents by priority, Count of closed incidents for the selected period by priority, Counts of active/closed incidents by service, Incidents SLA. * Incidents details   + Incident number, service, affected partners, ITSM system, priority, related assets, cause, impact, resolution, start date, resolution date, business outage duration, meeting/not meeting SLA, contact. * Delivery   + Average time to close incidents, Average time to close incidents variance. |
| OR4 | Service requests report. Offers an overview and details of the department’s service requests.  **Sections**   * Overview of service requests   + Count of active service requests by priority, Count of closed service requests for the selected period by priority, Counts of active/closed service requests by service * Service requests details   + SR number, ITSM system, summary, related assets, status, open date, close date, aging (days). * Delivery   + Average time to close requests, Average time to close requests variance. |
| OR5 | Change requests report. Offers an overview and details of the department’s service requests.  **Sections**   * Overview of changes   + Count of active change requests by priority, Count of closed change requests for the selected period by priority, Counts of active/closed change requests by service. * Change details   + Change number, summary, ITSM system, related assets, status, open date, close date, aging (days). * Delivery   + Average time to close change requests variance |
| OR5 | The reports can be viewed in full screen. |
| OR6 | The user can select and visualize a report from a list of reports. The list is expandable to add more reports as they are developed. |

# Appendix A: User authentication & Authorization Process



# Appendix B: News Types

|  |  |  |  |
| --- | --- | --- | --- |
| **Communique** | **Business Function** | Process | **Example** |
| [CIO Communiqués](https://plus.ssc-spc.gc.ca/en/page/communication-chief-information-officers)  l | Communiqués inform CIOs of service offerings or processes and when an action or response is required. They are prepared by various branches and are signed by ADMs. |  | [Example](https://service.ssc-spc.gc.ca/en/news/communiques/11-04-2024/ssc-deploy-outlook-mobile-secure-email-capability-important-actions) |
| [Infrastructure Change Notices (ICNs)](https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=32857257&logStopConditionID=2761849_1435436619_3_open) | This covers both types of ICNs:   1. Planned Infrastructure Changes: When a planned infrastructure change is scheduled, an ICN is sent to the impacted customer’s Deputy Minister (DM) and to the Chief Information Officer (CIO). 2. Emergency Infrastructure Changes: In the event of an emergency infrastructure change (less than 48 hours notice), an ICN is sent to the impacted customer’s DM and to the CIO. |  | [Example](https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=132745122) |

# Appendix C: Security Roles Requirements

The following table summarizes the **application security roles required**, based on the functional requirements. The actual role names will be determined in the [Drupal architecture and design document](https://163gc.sharepoint.com/:w:/r/sites/SGModernization/Shared%20Documents/Phase%204/Working%20Papers/Drupal%20Architecture/Serving%20Government%20Modernization%20-%20Drupal%20Architecture.docx?d=wdc49e851dcbc45cebdac2e18798b9b47&csf=1&web=1&e=kQr3o6).

|  |  |
| --- | --- |
| **Role** | **Description of Permissions** |
| Authenticated users (Member) | Employee of an organization that has been provisioned access to the site by an Organization User Manager (see below). Authorized Users must be associated with an Organization. Those with this status can login the authenticated section of the site.  Access is granted by the Organization User Manager. |
| Organization user manager | Authenticated SSC User with an enhanced role providing limited access to the Organization Module – Authorized User tab – in order to manage an Organizations list of authorized users. The Organization User Manager can add and remove users from the authorized user list only for their own organization (unless acting on behalf of another organization).  Access is granted by the Admin |
| Organization administrator | Authenticated SSC User with an enhanced role providing the ability to set attributes of any organization, add/delete new organizations, mark an Organization as onboarded as the ability to edit the ICN distribution list and authorized users for all organizations.  Access is granted by the Admin |
| ICN author | Authenticated SSC User with an enhanced role providing access to ICNs from the Content Module, which is required to create, edit, publish and delete ICNs.  Access is granted by the Admin |
| ICN distribution manager | Authenticated SSC User with an enhanced role providing access to the Organization Module – ICN Distribution List Tab which is required in order add/remove distribution list members for each organization.  Access is granted by the Admin |
| Content editor | Authenticated SSC User with an enhanced role providing access to the Content Module, which is required to add, edit, translate and delete Communiques as well as add and change content for the authenticated component of the site. The following exclusions/exceptions apply:   1. Content under the purview of the ICN Publishing Team 2. Content under the purview of the Organization user manager 3. Content under the purview of the Organization manager   Access is granted by the Admin |
| Administrator | This role should be exclusive to the team supporting the platform. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Persona** | **Site Content** | **CRUD** | **Description** |
| Authenticated User | Anonymous Section | Read Access | Any user attempting to access the site on a government departmental network can access the anonymous section of the site |
| User Profile | Read Access Update Access | Logged in Authenticated Users have access to view their profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Read Access | Logged in Authenticated Users have access to view their Organization Dashboard but do not have access to view any other organizations.  They do not have access to view any other organizations through the Organization Module and therefore cannot view the list of organizations, nor can they create, modify or delete an organization. |
| Communiques | Read Access | Logged in Authenticated Users have access to view, filter and search communications targeted to their organization  They do not have access to create or edit Communiques. |
| ICN | Read Access | Logged in Authenticated Users have access to view ICNs that have been issued for their Organization. They do not have access to create or edit ICNs. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| Organization User Manager | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Read Access      Update Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  Access to the Organization module to add/remove authorized users and only for their own organization. They do not have access to create/edit/delete an organization. |
| Communiques | Read Access | Access to view, filter and search communications targeted to their organization  They do not have access to create or edit Communiques. |
| ICN | Read Access | Access to view ICNs that have been issued for their Organization. They do not have access to create or edit ICNs. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| Organization Administrator | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their user profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Create Access  Read Access  Update Access  Delete Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  Full access to the Organization module to set attributes of any organization, add/delete new organizations, mark an Organization as onboarded as the ability to edit the ICN distribution list and authorized users for all organizations. |
| Communiques | Read Access | Logged in Authenticated Users have access to view, filter and search communications targeted to their organization  They do not have access to create or edit Communiques. |
| ICN | Read Access | Logged in Authenticated Users have access to view ICNs that have been issued for their Organization. They do not have access to create or edit ICNs. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| ICN Author | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Read Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  They do not have access to view any other organizations through the Organization Module and therefore cannot view the list of organizations, nor can they create, modify or delete an organization. |
| Communiques | Read Access | Access to view, filter and search communications targeted to their organization  They do not have access to create or edit Communiques. |
| ICN | Create Access  Read Access  Update Access  Delete Access | Logged in Authenticated Users have access to view ICNs that have been issued for their Organization. They do not have access to create or edit. Access to the Content Module for ICNs only to view, create, edit and delete ICNs. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| ICN Distribution List Manager | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their user profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Read Access      Update Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  They do not have access to view any other organizations through the Organization Module and therefore cannot view the list of organizations, nor can they create, modify or delete an organization. |
| Communiques | Read Access | Logged in Authenticated Users have access to view, filter and search communications targeted to their organization  They do not have access to create or edit Communiques. |
| ICN | Create Access  Read Access  Update Access  Delete Access | Logged in Authenticated Users have access to view ICNs that have been issued for their Organization. They do not have access to create or edit ICNs.   They also have access to the Organization Module but only the ICN Distribution list tab, allowing them access to add/remove users. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| Content Editor | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Read Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  They do not have access to view any other organizations through the Organization Module and therefore cannot view the list of organizations, nor can they create, modify or delete an organization. |
| Communiques | Create Access  Read Access  Update Access  Delete Access | Logged in Authenticated Users have access to view, filter and search communications targeted to their organization  They also have access to the Content Module to create, edit, and remove communiques and add/update/remove content on the site. |
| ICN | Read Access | Logged in Authenticated Users have access to view ICNs that have been issued for their Organization. They do not have access to create or edit ICNs. |
| Primary Reports | Read Access | Logged in Authenticated Users have access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They do not have access to modify the reports and/or data. |
| Admin | Anonymous Section | Read Access | Access to the anonymous section of the site |
| User Profile | Read Access Update Access | Access to view their profile and update only their contact and professional information (Job Title and Role) |
| Organizations | Create Access  Read Access  Update Access  Delete Access | Can view their own Organization Dashboard but do not have access to view any other organization dashboard and cannot edit the page.  They also have full access to the Organization Module and can create, edit and remove an Organization including adding authorized users. |
| Communiques | Create Access  Read Access  Update Access  Delete Access | Access to view, filter and search communications targeted to their organization  They also have full access to the Content Module and can create, edit and remove any type of content. |
| ICN | Create Access  Read Access  Update Access  Delete Access | Access to view ICNs that have been issued for their Organization. They also have full access to the Content Module and can create, edit and remove ICNs and add/remove users to the ICN distribution list. |
| Primary Reports | Create Access  Read Access  Update Access  Delete Access | Access to view and filter pre-determined PowerBI reports belonging to the users’ organization.  They have access to create elements of the primary reports but cannot change its data |
| People/Roles | Create Access  Read Access  Update Access  Delete Access | Access to add/remove users to the site, assign and update roles. |

1. This is for MVP only and will be evolved post MVP with multiple roles allowing different levels of access. [↑](#footnote-ref-2)