Accessibility

Assigned

Reviewer: Accessibility Self-Attestation Last activity: Oct 9, 2025, 12:01 PM

R: 0/2 (0%)

T: 0/2 (0%)

Hide All Details

R: Accessibility Awareness

T: Plan for accessibility

If you are planning to distribute your project to a wide audience in a future release, you should plan for, and start building in, accessibility support early to prevent costly re-work in your project schedule.

By including accessibility support now, you will speed up the accessibility review that is required when you release your project broadly.

- Review the Accessibility Quick Reference Guide to learn about how to design and develop for in your product.

The Accessibility team is available for early consultation which can be very helpful in preventing bugs and rework later in your development cycle. If you would like a consultation, post a message to the **Message Board** with the subject "@Accessibility: Consultation" and they will schedule a time to meet with you.

R: Accessibility Self-Attestation

T: Validate Accessibility task completion

Complete the above Accessibility tasks and then check off this task to self-attest that you have done this work to meet the Microsoft Accessibility standards. No further Accessibility review or sign-off is required.

Important

ID 9511: MSR Event Agent... Processing Active Overall Task Status 8/25 (32%) Peter Salhom (Stron...

Naming

Approved

Reviewer: Simon Farr Last activity: Oct 21, 2025, 12:11 AM

R: 1/1 (100%)
T: 1/1 (100%)

Hide All Details

R: Temporary Code Names Must Follow Guidance

Simon Farr
10/21/2025, 12:11:24 AM

T: Select an appropriate code name

Jeff Running
10/9/2025, 12:02:01 PM

1. Use the Codename Request Tool to select an appropriate temporary/working code name for your project.

   Note: Do not use the term "GPT" in your project name and code.

2. Provide the name you have selected in the *Naming & Trademark : Final Code Name* metadata field.

   - Click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.

Note: CELA does not review internal codenames, temporary project names, or other names that are for internal use only.

Privacy

Waiting On Submitter

Reviewer: Kelly Mason Singh (SHE/HER) Last activity: Oct 21, 2025, 10:13 AM

R: 0/5 (0%)
T: 1/5 (20%)

Hide All Details

R: Data Retention and Deletion

Important: Only collect data that is expressly needed and substantiated by a *legitimate business purpose*.

2. Complete the data retention information requested in the template.
3. Work with your Privacy SME to determine if the data you are collecting should be considered sensitive and therefore should have a shorter retention period.
4. Attach the completed DIRP to this task.
    - Click the paperclip icon to the right of the Task title above and select the document you wish to attach. Click the "+" icon to add additional attachments. **Details:** How to add an attachment.

For an Update Record (an update to a previously released project):

1. Review and update your DIRP from the previous release to ensure that it is complete and accurate, and verify that you are following it.
2. Review and update your service or app Data Grid registration and tagging to ensure if reflects any changes in your data inventory.
3. Attach a copy of the updated DIRP to this task as evidence.

R: Internal Communications

T: Verify that internal communications follow guidance

Jeff Running
10/18/2025, 5:11:02 PM

Internal email must:

1. Be sent from and show a valid Microsoft-owned domain email address.
2. Include an introduction to identify the sender and the relationship (e.g., "As a past participant in our research studies...").
3. Include a footer with the following:
    1. A link to opt-out of future emails. This can best be accomplished by using one of the approved tools below or a Distribution List that individuals can join or leave. See //idweb for more info. Suggested text: "If you prefer to not receive research communications, click here <link> to remove your name from my list."
    2. A signature block with the sender's name (team), a link to the internal Privacy Statement

Note: Marketo is not approved for mails to FTEs globally. Email tracking of employees is prohibited. If you want tracking, you should consider anonymized using PoliteMail.

R: Notice and Consent for User Experiences Custom

T: Provide a clear notice and obtain consent

Important: To be valid, consent must be 'freely given, specific, informed, and unambiguous' **and** data may not be collected until affirmative consent is provided.

1. Provide a prominent notice that describes the types of personal data you are processing and which provides opt-in consent and user controls.
2. Provide users with a way to revoke or modify any consent given, where the use requires opt-in or opt-out consent.
3. Provide the URL to the Notice & Consent statement in the *Privacy : Notice & Consent Location* metadata field.
    - Click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.
4. Attach a screenshot to this task showing the Opt-Out options that will be provided.
    - Click the paperclip icon to the right of the Task title above and select the document you wish to attach. Click the "+" icon to add additional attachments. **Details:** How to add an attachment.
5. If you are collecting sensitive data, attach a screenshot to this task showing how you are providing explicit consent.
6. If you are collecting data that is not obvious to the user, or is not covered by the Privacy Statement, create a First Run Experience (FRE) that provides notice about the data that will be collected, and how it will be used.

   An FRE is considered a best practice and a mechanism for obtaining unambiguous consent.
7. Attach a screenshot to this task showing how users will be able to revoke and modify consent.

R: Privacy Statement

- Include a link to the Microsoft internal Data Privacy Notice (DPN)
- Use this forward link: http://go.microsoft.com/fwlink/?LinkId=518021
- Label the statement “Data Privacy Notice”

- **For projects intended for individuals outside of Microsoft:**
  - Include a link to the Microsoft Privacy Statement
  - Use this forward link: https://go.microsoft.com/fwlink/?LinkId=521839
  - Label the statement "Privacy & Cookies"
- **If your project collects consumer health data:**
  - Include a link to the Consumer Health Privacy Statement
  - Use this forward link: https://go.microsoft.com/fwlink/?linkid=2259814
  - Label the statement: “Consumer Health Privacy”
  - Suggested placement: near the “Privacy & Cookies” link
- **For external Source Code releases:**
  - Include a link to the Microsoft Privacy Statement in your Readme file.
  - Use this forward link: https://go.microsoft.com/fwlink/?LinkId=521839.
- **For websites:**
  - Follow the Privacy Website Guidance information on how to create the web page footers and link to the appropriate statement.
- **For WeChat Apps:**
  - The Privacy Statement link may be added to the Welcome text displayed in the Chat screen when opening the Official Account.

    If there are multiple apps with different Privacy Statements in the Official Account, display the Privacy Statement within each app.

    Note: Custom Privacy Statements must be approved by CELA Regulatory Affairs and localized into the languages into which the release will be localized.

2. Follow these additional requirements:
   - If the release provides pop-ups that collect data then the privacy statement may need to be displayed on the pop-up itself.
   - If the release is designed for a small screen it is sufficient for the privacy statement to be accessible from the "hamburger menu".
   - If the release will be localized for South Korea, use a localized link label: "개인정보처리방침" (Korean for "Privacy Statement").

ID 9511: MSR Event Agent... Processing Active Overall Task Status 8/25 (32%) Peter Lawrom (Stron...

T: Make sure authentication meets data collection and data subject rights obligations

Authentication mechanisms must meet Microsoft obligations for data collection, consent, and data subject rights.

If you are using Microsoft account (MSA, formerly Windows Live ID):

- You must use the same form of verification to initially identify a user's age, region, and country to products that rely on this information for credentialing.

If you are using a non-Microsoft authentication method (e.g., AppleID, Facebook, Gmail, or others):

- You must obtain the necessary information and support from the authentication entity for Microsoft to meet its privacy obligations, including obtaining parental consent where appropriate, supporting the privacy choices of our users and adherence to our security requirements.

Publishing

Approved

Reviewer: Nisha Godha (DESIGN LABOR... Last activity: Oct 20, 2025, 5:16 PM

R: 1/1 (100%)

T: 1/1 (100%)

Hide All Details

R: Publishing a Website

Nisha Godha (DESIGN LABORATORY INC)

10/20/2025, 5:16:25 PM

ID 9511: MSR Event Agent... Processing Active Overall Task Status 8/25 (32%) Peter Salhan (Stron...

- The final URL that will be used once your release is live in the *Publishing : Web Final URL* metadata field.

To add metadata, click the Metadata icon (<M>) to the right of the Task title above and enter the values in the appropriate fields. **Details:** How to add metadata.

Responsible AI

Approved

Reviewer: Brenda Belcher Last activity: Oct 29, 2025, 4:31 PM

R: 3/3 (100%)
T: 3/3 (100%)

Hide All Details

R: Provide Additional Information to Responsible AI Reviewer

Brenda Belcher
10/15/2025, 11:38:10 AM

T: Provide additional information for the Responsible AI review

Jeff Running
10/14/2025, 7:07:46 PM

To help the Responsible AI (RAI) reviewer determine the applicability of RAI requirements:

1. Please initiate a dialog with the RAI reviewer, either over the Message Board or by signing up for T&R Office Hours (aka.ms/trofficehours).
2. Provide relevant information on:
   - the specific use of the generative capabilities of the AI code/model/demo
   - the sensitivity of its potential uses

Based on the information provided, one or both of these additional requirements may be assigned:

Deployment Safety Board (DSB): DSB review and approval (aka.ms/tnrdsb) is required for releases involving generative models.

Sensitive Uses (SU): Microsoft requires that potentially sensitive uses of Artificial Intelligence be reviewed by the Office of Responsible AI (aka.ms/sensitiveuses).

You can advance the review process more quickly by clearly addressing the generative capabilities and any sensitive applications of your model in this initial communication.

ID 9511: MSR Event Agent... Processing Active Overall Tas' Status 8/25 (32%) Peter Salvitti (Stron...

We need to know specifically what you are releasing (code, model, data, demo, product, etc.) and to where (GitHub, Hugging Face, Azure Model Catalog, etc.) in order to point you to the right template. Review this record to be sure you have provided this information accurately and completely.

1. Review the latest information at: aka.ms/tnrtransparencydocs.

   If you have previously created transparency documentation, the guidance and templates may have changed.

2. Follow instructions from the T&R RAI team (see the RC&ET Message Board) to locate the recommended template for completing your transparency documentation.

3. Without moving it, complete the transparency documentation template(s) recommended by the T&R RAI team.

   Leave your document(s) in the shared folder we create to facilitate feedback and tracking.

4. Let us know over the Message Board when your draft is ready for review.

5. Respond to SME feedback.

Once your record is approved, share your transparency documentation with users together with your release. For example, in GitHub, use it as your README or share it separately as transparency.md in the root directory.in the root directory.

Note: You may check off this task once you have completed your draft. However, please remain engaged over the Message Board, as the requirement can only be approved after any requested revisions have been made and accepted by both you and the assigned RAI SME.

R: Impact Assessment Custom

Brenda Belcher
10/15/2025, 11:38:04 AM

T: Complete an Impact Assessment

Brenda Belcher
10/15/2025, 11:37:59 AM

1. Follow instructions from the T&R RAI team (see the R&CT Message Board) to locate the recommended template for completing your impact assessment.

2. Without moving it, complete the impact assessment template recommended by the T&R RAI team.

   Leave your document in the shared folder we create to facilitate feedback and tracking.

3. Let us know over the Message Board when your draft is ready for review.

ID 9511: MSR Event Agent... Processing Active Overall Task Status 8/25 (32%) Weak (Strong...

previously created an impact assessment, the guidance and templates may have changed. Please review the latest information.

Security

Assigned

Reviewer: Ellyse Mooney Last activity: Oct 21, 2025, 10:11 AM

R: 0/8 (0%)

T: 2/13 (15%)

Hide All Details

R: Core Security: Release Planning and Preparation

- [ ] T: Create or update a threat model

We recommend using the Threat Modeling tool because it has build-in analysis for commonly used system components, However, you need not run the analysis. For smaller systems, threat models can also be created in Visio, PowerPoint, or Paint.

1. Download the Threat Modeling tool from aka.ms/threatmodelingtool.

   Step-by-step guidance for creating a threat model and our expectations are documented at https://aka.ms/TnR/ThreatModeling. For detailed information, see the Security Engineering Threat Modeling topic.

2. Create a threat model for your release.

3. Attach the completed threat model to this task.

   - Click the paperclip icon to the right of the Task title above and select the document you wish to attach. Click the "+" icon to add additional attachments. **Details:** How to add an attachment.

4. If your app requires AAD/O365 tenant level permissions, then visit https://aka.ms/TnR/AADReview and create a ticket to schedule an AAD permission review.

   Please invite @TnRSecurity to the meeting and keep a list of permissions and the threat model ready for the review.

1. Place the source code in an approved managed source repository.

   If you are releasing source code to the general public, during development make all changes in a private repository in GitHub. After you receive final approval in *Release, Compliance & Ethics Tracker*, you may publish your project to a GitHub public repository located under the https://github.com/microsoft organization.

   If you are not releasing source code to the general public, use an approved Visual Studio account. In most cases, that account will be *msresearch.visualstudio.com*.

   See the Handling Source Code How-To on the T&R Security SharePoint site for more information.

2. Provide the full URL / path to your code repository in the *Security : Primary Code Repository Path* metadata field.

   - Click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.
   - To add additional repository paths, click the '+' in the Metadata pane and add additional *Security : Secondary Code Repository Path(s)*entries.

3. Grant the T&R Security team access to the code repository:

   - For GitHub - Grant Administrator access to the microsoft/TNRSecCompliance team
   - For Azure DevOps - Add the "T+R Security" (TnRSecurity@microsoft.com) security group as a member of project Administrators

   Important: Make sure the repository restricts access to authorized Microsoft personnel only.

For releases that include a data model

- Provide the URL paths for the AI or ML Foundry experiment and job that produced the model being released. These should be available from your ML experiments dashboard:
  - What *Experiment and Job* produced the model? Provide the full URL / path to your code repository in the *Security : Primary Code Repository Path* metadata field.
    - Click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.

      To add additional Jobs/experiment paths, click the '+' in the Metadata pane, select *Security : Secondary Code Repository Path(s)*, and then provide the path(s).

1. Follow Microsoft corporate standards to provide an authenticated user experience:
    - Use Only Approved Microsoft Account SDKs, Interfaces and Authentication Policies
2. Follow safe operating procedures for managing your identity to access the application back-end for operating, troubleshooting, and testing.
3. Take care to procure and properly handle service accounts required to run the service.
    - Accounts must meet Identity Management Baseline requirements

T: Use only approved non-people identities

Jeff Running
10/14/2025, 7:11:43 PM

1. **Ensure No Issues in S360:** Check that there are no issues in the S360 Certificates and Secrets Management KPI.
2. **Follow Security Team Activities:** Adhere to the activities defined by your Security Team as identified in the Service Tree (XDiv SecurityTeam).
3. **Implement Managed Identities:** Use Managed Identities for services that support Entra ID authentication. Ensure user-assigned identities are preferred over system-assigned identities.
4. **Role Assignments:** Delete role assignments when Managed Identities are deleted and isolate user-assigned identities between environments.
5. **Service Principals:** Ensure Entra ID app Service Principals are not listed as Admins within their own Service Tree entries.
6. **Accountable Owners:** List at least two Microsoft Full-Time Employees (FTEs) as accountable owners/sponsors in Entra ID for non-people identities.
7. **Secret Management:** Change the initial secret of non-people identities before first use and follow the Secret Storage & Credential Management Requirement.
8. **Expiration Date:** Set an expiration date of 180 days from the creation date for non-people identities, renewable by an owner.
9. **Restrictions:** Ensure non-people identities are not enabled for Remote Access Services (RAS), do not resemble individual user identities, and are not allowed local or remote interactive logon.
10. **Minimum Privileges:**
    - Assign only the minimum level of privileges needed for non-people identities to accomplish required tasks

1. You must run/enable the following source code analysis tools:
    - **Azure DevOps**
        - Credential Scanner
        - CodeQL
        - Component Governance

          Note: Component Governance can detect Python packages from requirement files but cannot detect components from Conda environment definition files. For Anaconda packages create a manifest file with details of components. A sample manifest file and schema is outlined in the Static analysis documentation.
        - Component Governance for Containers

          If your repository hosts or builds docker/container images, then add another instance of the Component Governance build task with the path of the image.
    - **GitHub**
        - Secret Scanning (enabled by default for repositories under Microsoft organization)
        - CodeQL Action
        - Dependabot for Component Detection

    Important: Ensure external packages (NPM, Nuget, Maven, and Python) are referenced from a secure location. Validate the package risk level here.

    This guidance is also applicable for secondary builds.
2. The easiest way to run these tools is to add them in your build pipeline in a Microsoft-managed Azure DevOps account or on GitHub.

    You can decide to add these tools to an existing pipeline or create a new dedicated static analysis pipeline.

    To create a build pipeline and analyze results, see: Static analysis.

    For a sample YAML pipeline, see: aka.ms/TnR/SampleBuildPipeline.

    For CodeQL onboarding guidance based on your build process, see: CodeQL | 1ES On EngHub.

    - **Azure DevOps**

- Preferred: Create a build pipeline on Azure DevOps and use GitHub repository as source.
- Enable tools, actions, and options on GitHub; doesn't required a complementary Azure DevOps project.

  This option doesn't raise errors for licensing incompatibility.

3. Resolve all security errors and warnings.

   How to check for reported problems and what to look for in logs is documented in the Static analysis documentation.

4. Schedule the build pipeline to run automatically once a week.

   Note: It must be connected to the master branch.

5. Provide the full URL / path to your latest successful build logs in the *Security: Primary Latest Successful Build Logs Path* metadata field.

   - **Azure DevOps:** Provide the build log URL.

     Make sure the retention of build is set to at least 180 days or at least 30 days beyond the release of the record, whichever is later.

   - **GitHub:** Provide a URL of CodeQL Action run/output and a link to Dependabot/Security Advisories.

     If the link doesn't point to a specific instance, then attach a screenshot.

   - To add metadata, click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.

     If you have more than one repository, provide the URL / path to the latest successful build log for each additional repository: click the '+' in the Metadata pane, select *Security : Secondary Latest Successful Build Logs Path(s)*, and then add the additional path(s).

If you have questions, contact the Security SME assigned to your record for help in triaging open issues by adding a message with subject "@Security:" to this task.

R: Core Security: Baseline Cryptography

A list of Crypto Board approved libraries is available at: https://aka.ms/sdl-encryption-spreadsheet

3. If you have questions about your encryption implementation, please contact the Security SME assigned to your release as soon as possible by posting a message to the Message Board with the subject "@Security".

4. If you have specific questions about a crypto library or you are implementing your own crypto algorithms, then please drop an email to the Crypto Board (cryptobd@microsoft.com) and schedule an algorithm review. Keep @TnRSecurity in the loop for all conversations.

Note: Certain encryption models and algorithms are *Not Approved* for use by the SDL requirements and may require Crypto Board review for approval. Please contact the Security SME assigned to your release for review and details.

☐ T: Configure source feeds

All products and services using a mix of internal and external package dependencies must configure source feeds (such as NuGet, NPM, or PyPI) to retrieve dependencies only from approved software repositories.

- Provide the path to your Azure Artifacts feed in the *Security : Azure Artifacts Feed* metadata field.
    - Click the Metadata icon (<M>) to the right of the Task title above and enter the value in the appropriate field. **Details:** How to add metadata.

R: Enterprise Application: Azure/Office Consent Requests

☐ T: Assign SC-Alt accounts as owners

All application owners must be SC-ALT accounts and all configurations of the application/service principal must be performed using a SAW.

Applications must have at least two owners, at least one of whom must be an FTE.

1. Navigate to the Azure Portal and go to Enterprise Applications.

   Ex: https://portal.azure.com > More Services > Identity > Enterprise Applications.

ID 9511: MSR Event Agent... Processing Active Overall Tas' Status 8/25 (32%) Peter Warm (Stron...

restricted to only the users who need to use the application.

1. Navigate to Azure Portal and go to Enterprise Applications.

   Ex: https://portal.azure.com > More Services > Identity > Enterprise Applications.

2. Select 'All applications' on the navigation pane on the left and search for your application.
3. Go to Properties on the left menu.
4. Toggle 'Assignment Required?' to Yes.

☐ T: Set a valid Reply URL

All enterprise applications must have a valid reply or redirect URI, registered and owned by Microsoft.

1. Navigate to Azure Portal and go to App Registrations.

   Ex: https://portal.azure.com > More Services > Other > App Registrations.

2. Search for your application under Owned applications.
3. On the Overview pane, click on the 'Add a Redirect URI' link to add a redirect URI.

   It must point to your Web App or any valid website.

☐ T: Review Admin Consent requirements

1. Review Admin Consent Requirements on: https://aka.ms/TnR/AdConsentRequirements.
2. Review the risk associated for all permissions requested by the enterprise application by visiting the PowerBI report.

   Most delegated permissions with low to medium risk will get approved. Requests for Admin privileges will be rejected.

3. Submit an Admin Consent Request: http://aka.ms/ACEAADReview

R: Online Web Release: Access Controls

ID 9511: MSR Event Agent... Processing Active Overall Tas' Status 8/25 (32%) Weaker Warm (Stron...

4. Take the required actions to protect secrets (keys, passwords, and other kinds of stored secrets) prior to deployment.

   See the Help for more details.

R: Online Web Release: Encryption Controls

T: Handle all communications securely with the right level of encryption

If you are publishing to an internal audience only and do not need a custom domain name for your website, then enable the default HTTPS configuration.

Azure Web applications support HTTPS natively:

1. Navigate to the Web App in Azure Portal.
2. Select 'TLS/SSL settings' under 'Settings' on the navigation bar on the left.
3. Set 'HTTPS Only' to On and 'Minimum TLS Version' to 1.2.

If you are publishing to an external audience and need a custom domain name for your Azure Web application, or if you are hosting your website on a virtual machine, then you must request a certificate from OneCert.

Request a OneCert Certificate:

1. Create an SSL certificate for your site, using OneCert. For instructions on migrating a certificate from SSLAdmin to OneCert see: SSLAdmin Migration to Microsoft PKI.
2. Ensure you have configured your site cookies for HttpOnly, and that it requires Secure Cookies.
3. Ensure your site is enforcing TLS 1.2 and is configured to limit use of deprecated ciphers.

To use the certificate with Azure Web application:

1. Navigate to 'TLS/SSL settings' under 'Settings' for the web application, on the navigation bar in Azure Portal.
2. Click 'Add TLS/SSL Binding' and upload your certificate.

Release, Compliance & Ethics Tracker : Activity Center

ID 9511: MSR Event Agent...	Processing	Active	Overall Tac' Status	8/25 (32%)	Waterfall (Stron...