Copy of Azure AD Application Request Fulfillment Process

NOTE: This is a copy of the original document. This copy is intended for those outside the Microsoft Infrastructure service team to reference.

Status: Production (prior version of this document)

Existing version of this document will become production on 1/11/2017

Purpose

A request fulfillment process for handling MI requests for Azure AD applications with risky permissions.

Goals

1. Enable business use
2. Show due care for integration with UW confidential data

Roles

The following parties are involved in this process. Listed by name, role, and responsibilities.

Name	Role	Responsibility
Customer	Requestor	Submit the request for Azure AD application with sufficient information needed by approvers.
MI Support	Coordinator	Support the requestor through this process.
MI Engineering	Authorizer	Configure/create application if the request is approved.
AAD App Risk Scoring Team	Assessor	For approvals, assess application as fit for use, identifying potential/necessary mitigations so applications are fit for use
AAD App Risk Review Team	Reviewer /Consultant	On a periodic basis, review applications for risk. On an as needed basis, provide consulting on application risks and suggested mitigations.
MI Service Manager	Approver	For basic approvals, approve application as fit for use. For extended approvals, taking risk assessment and ensuring any necessary mitigation is applied to applications before approving application for use.

The MI Support role is filled by the service team members.

The MI Engineering role is filled by the service team engineers.

The AAD App Risk Scoring team is:

- Eric Kool-Brown
- Shawn Drew
- Jonathan Pass
- Roland Lai

The AAD App Risk Review Team is filled by a representative from the Attorney General's Office, Office of the CISO, and Risk Management.

The MI Service manager is filled by the service manager or their designated alternate during leave.

Entry criteria

1. Applicant submits MI Azure AD Application Request Form resulting in a new UW Connect record.
2. The UW Connect record is assigned to CI=Azure AD, Assignment Group=Microsoft Infrastructure.

Process steps

1. MI Support reviews the customer's request for required information:
    a. Verify the Type of AAD application is provided.
    b. Verify the Access to other AAD applications being requested is described sufficiently that we know what the client is requesting.
    c. Verify the Business Need is described.
    d. Verify the Data Use & Exposure is described.
    e. Coordinate with Customer to ensure all required information is available for approvers.
    f. If necessary, add application in dogfood tenant to determine any unclear information and/or clarify with the customer anything missing or unclear.
    g. When required information is provided, coordinate expectations with Customer: you're now moving on to the approval stage.

2. MI Support passes the baton to a member of the AAD App Risk Scoring Team:
    a. MI Support creates a RTASK assigned to a member of the AAD App Risk Scoring Team. Description should clearly say "we have a risky AAD app which needs analysis for approval".
    b. RTask owner on AAD App Risk Scoring Team notifies AAD App Risk Scoring Team about need to review app
    c. AAD App Risk Scoring Team reviews details provided, does whatever activities are needed, and renders a decision. That decision may include conditional approval pending mitigations. NOTE: If there is a clear service manager/owner, system manager/owner, or data custodian representing the AAD application permission that the requested risky AAD app needs, then that individual can/should be approached to make a risk acceptance decision. In that case, no decision is needed from App Risk Scoring team, and in step #4 we open a routine change which does not need CAB approval. For example, if application Q wanted Directory.Read.All, the MI service manager could make a decision. If application J wanted OneDrive.SpecialAdminPermission (there is no such thing), the MSCA service manager could make a decision.
    d. RTask owner documents decision and the rationale behind that decision and any suggested mitigations for historical review.
    e. RTask owner communicates decision. If discussion is needed, coordinate and facilitate mitigation discussion.
    f. RTASK is marked complete.
3. MI Support reviews decision on whether to proceed with approval
    a. MI Service Manager discusses potential mitigations with requestor to identify if they are acceptable.
    b. If an application has acceptable risk it is approved
4. MI Service Manager send app approval to AAD Change Advisory Board for additional decision. NOTE: if in 2c the risk was accepted by a specific owner/manager/steward, then a routine change is open, approved, and no decision by the CAB is needed.
    a. AAD CAB supplies its own process for reviewing app approvals. Note
    b. If approved, move on to #7.
    c. If denied, service manager reviews concerns and may start over at a prior step or communicate denial to customer.
5. Request owner coordinates access with MI Engineering.
    a. Ask MI Engineering to add requested AAD application.
    b. MI Engineering adds requested AAD application.
    c. MI Support updates MI AAD Apps - Fulfilled Requests Azure AD Application - Fulfilled Requests
        i. Record the Application that was authorized and the requestor.
        ii. Record the access granted.
        iii. Record the UW Connect record number tied to the request and approvals.
        iv. Record the status of the request.
        v. Record the data exposure.
        vi. Record any required mitigations
        vii. Record the approval date.
        viii. Record notes as needed.
        ix. Save.
6. MI Support responds to Customer: You're good to go.
7. MI Support resolves UW Connect record.