

Service Area Risk Assessment

Service Area: Authentication and Directory Services

Author: Al Lilianstrom

Date: Sept. 26, 2016

The purpose of this document is to consider, analyze and record risks to the delivery or operation of services. This analysis is to be done annually, or more frequently if there are potentially significant changes in business, technical, regulatory, security or financial conditions.

The Service Area owner shall consider risks to meeting Service Level Commitments. Consider whether the dependencies on other services and underpinning contracts pose new risks.

1. Lab and Customer environment
 - Denial of Service attack from onsite system
 - Misconfigured Service Provider locking accounts in central authentication
2. Availability and Continuity
 - FCC2 Computer room extended outage
 - Master KDC offline – no password changes or new accounts in Kerberos realm
 - Possible LDAP service usability issues
 - DNS update required to correct
 - Active Directory Domain Controller offline
 - If FSMO role holder issue may arise depending on length of outage
 - FCC3 Computer room extended outage
 - Possible LDAP service usability issues
 - DNS update required to correct
 - Active Directory Domain Controller offline
 - If FSMO role holder issue may arise depending on length of outage
 - WH8FC Computer room extended outage
 - Possible LDAP service usability issues
 - DNS update required to correct
 - Active Directory Domain Controller offline
 - If FSMO role holder issue may arise depending on length of outage
 - Core network outage
 - All computer rooms offline
 - All authentication services unavailable
 - Power Outage and Generator failure
 - All Authentication Services offline after UPS battery runs out
 - F5 Load Balancer outage
 - Service Providers using LDAP Service could see problems with authentication

- Federation Services offline
- Central VM Infrastructure outage
 - Federation service offline
 - APPS domain offline
 - RSA service offline
 - Eduroam service offline
- DNS Outage
 - Active Directory authentication problems
 - LDAP Service authentication problems
 - Kerberos authentication problems
- External Vendor
 - CRL for valid users
 - Not able to issue/revoke cards

3. Capacity

- Server overload
 - Kerberos
 - Automatic failover to next responsive KDC
 - Active Directory
 - Automatic failover to next responsive Domain Controller
 - LDAP Service
 - Automatic failover to next responsive Domain Controller for internal SERVICES domain Service Providers
 - LDAP Service Providers using SERVICES.FNAL.GOV may experience authentication failures
 - LDAP Service Providers using LDAPS.FNAL.GOV will failover to the other domain controllers
 - APPS Domain
 - Automatic failover to next responsive Domain Controller
 - Eduroam
 - Automatic failover to next responsive server
 - RSA
 - Authentication failures may occur
 - Federation Service
 - Automatic failover to next responsive server
 - PIV-I
 - No special considerations

4. Incident and Request Response and Resolution

- Slow ticket response
 - Server offline – authentication impacted
 - Server overloaded - authentication impacted
 - Account availability – user(s) not able to do their activities

5. Security

- Zero day threat takes systems offline
 - All authentication for impacted service stops

6. Financial or Contractual

- Expiration of Microsoft support agreement
 - Active Directory
 - LDAP Service
 - APPS
 - Eduroam
 - Federation Services
- Expiration of Dell hardware support agreement
 - Active Directory
 - LDAP Service
 - Kerberos
- Expiration of Ping Identity support agreement
 - Federation Services

Recommendations:

for changes in Service Levels or risk mitigation actions, other than those already considered and accepted as part of the annual budget process (such as staffing levels)

Version history

Version	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0					
2.0	Al Lilianstrom	9/26/2016			Add PIV-I
3.0	Al Lilianstrom	2/14/2017			Remove KCA
4.0	Al Lilianstrom	5.22.17			Annual review chg12862. No changes.
5.0	Al Lilianstrom	10/1/2018			Annual review. No Changes
6.0	Saul Gonzalez	7/10/2019			Annual review. No Changes.
6.1	Saul Gonzalez	3/16/2020	CHG000000 017343		Annual review. No Changes.

Next revision date: 10/2021