**May 29, 2020 - BCBS of AZ Disaster Recovery (DR)**

**Table Top Exercise**

**Comm Vault- DR Plans Review/Planning Workshop Meeting**

Agenda

o   **Overview & Goals of the Planning Workshop Meeting (s)**

To either review existing legacy DR Plan (DRP) documentation, Run Books, etc., or engage in workshop style-discussion geared to pulling together data/processes for creation of a suitable DRP. Details regarding the DRP requirements-gathering are covered later within agenda. Once finalized, this plan will be reviewed and walked-through as part of the subsequent Table Top DR Exercise (simulating a failover to RDC).

Between now and May 29, we’ll use our time to discuss DR strategy and to document the strategy and requirements into a suitable DRP.

The DRPs should be **finalized at least 2 weeks prior to** the DR Exercise Date (5-29-20). A meeting will be scheduled to walk through the completed DRPs (called, ***“Final Walkthrough Meeting”).*** This final TEAM meeting will be scheduled approximately 2 weeks prior to the DR Exercise Date.

o   **Recovery Scope (apps in scope)**

|  |  |
| --- | --- |
| **May 29, 2020 DR Exercise Components in-scope and owners** | |
| **Component** | **Owner** |
| Cisco ESA (IronPort) | ISS- Sweeney |
| Force point (Web Sense) | ISS- Sweeney |
| Sentinel | ISS- Sweeney |
| Microsoft PKI | ISS- Sweeney  Server Services- Nelson |
| FireEye (to be phased out- req. offline discussion) | ISS- Sweeney |
| Sophos | ISS- Sweeney |
| Cyber Ark | ISS- Sweeney |
| Cisco FTDs | Network- Zwoyer |
| Extra Hop 7.2 (to include **DHCP/DNS** in scope of discussions) | Network- Zwoyer |
| Extra hop ‘Reveal X’ | ISS- Farr |
| SCCM (integrated with ‘In Tune)’ | Cloud Services-Eggert  Desktop Services- Darner/Sipos |
| Comm Vault | Operations- Hall |
| System Center Operation Manager (SCOM) | Operations- Hall |
| Splunk | Operations- Hall |

o   **Recovery Planning Checklist (to be reviewed at workshop)-**

Using the example Disaster Recovery Plan (DRP) as a guide, please describe the following (and provide supporting detail to define for your specific app/component).

* + Who is the owner and responsible person for the integrity of this DRP?
  + Whom are the necessary Support Team members to recover & activate this app within a DR mode of operation (failed over to RDC site)?
  + Skill set/permissions/support tools required? Team Member name?
  + How are these persons kept in contact while performing DR (contact information)?
  + What DR hardware is required to activate the recovered application at RDC?
  + What is the actual Recovery Process to render the RDC systems recovered and operational?
  + What are the Validation Steps which will be used by testers/users to validate (accept) that the recovered systems are operational?
  + What dependency applications need to be available to enable full functionality for this application? Describe upstream (feeds your system) and downstream (consumes your output and services) and also describe the Recovery Time Objective (RTO) for those dependencies.
  + Please describe the overall operation of this component and how used.
  + How will recovery issues be noted/tracked/resolved/reported during the Table Top DR Exercise.
  + Other topics pertinent to the recovery and full functionality of DR.