# **Introduction**

The following provides a companion narrative to the ‘BCF Process Overview Flowchart’. Here we will provide a brief explanation for each element in the process. By way of convention, items that are underlined have a corresponding document name in the framework.

# **Discovery**

The Discovery process uses various technical tools to gather information about all of the systems in your corporate environment's various networks and IaaS clouds. The information-gathering process should result in a comprehensive list of systems in the corporate environment. It often highlights those systems thought to be ‘retired’ but may still be active on your network. This information will drive the ‘Risk Analysis’ process. Steps in this process include:

|  |  |  |
| --- | --- | --- |
| Process Name | Description | Example Tool |
| **Authenticated Vulnerability Scan** | A network vulnerability scan that is configured to ‘log in’ to assets being scanned to produce more accurate and comprehensive insight into its security posture | * [Qualys](https://www.qualys.com/scanning-accuracy/) [Rapid7](https://www.rapid7.com/solutions/network-vulnerability-scanner/) * [OpenVAS](https://www.openvas.org/) |
| **CMDB Export** | An export from the configuration management tool that includes information around hardware age, support contract status, business unit, location, etc. | * [ServiceNow CMDB](http://www.servicenow.com/products/cmdb.html) [BMC Helix CMDB](http://www.bmc.com/it-solutions/helix-cmdb.html) * [i-doit CMDB](https://www.i-doit.com/) |
| **XDR Export** | A status report for all systems in the Extended Detection and Response system | * [Microsoft Defender](https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-xdr) * [SentinelOne](https://www.sentinelone.com/) * [CrowdStrike](https://www.crowdstrike.com/platform/endpoint-security/) |
| **Backup Reports** | Reports on backup status and history for all systems | * [Datto](https://www.datto.com/) [Carbonite](https://www.carbonite.com/) * [Bacula](https://www.bacula.org/) |
| **Change Management Exports** | An export from the change management database for all system names under the scope of the change management process | * [ServiceNow Change Management](https://www.servicenow.com/products/change-management.html) * [SolarWinds Service Desk Change Management](https://www.solarwinds.com/service-desk) * [Rundeck](https://www.rundeck.com/open-source') |
| **Configuration Management Reports** | An export from the configuration management database for all system names under the scope of the configuration management process | * [Puppet Enterprise](https://puppet.com/products/puppet-enterprise) * [Chef Automate](https://www.chef.io/products/chef-automate) * [Terraform](https://www.terraform.io/) |

# **Risk Analysis**

The System Risk Analysis process assesses the risk posture of the systems based on the compiled inventory and identified vulnerabilities. The data gathered in the previous step will be fed into the *BCF - System Risk Analysis Spreadsheet.*

|  |  |  |
| --- | --- | --- |
| Process Name | Description | Output |
| **Compile / Analyze Process** | Manually review the output of each of the processes listed above for completeness and accuracy | Re-initiate any failed process until the output matches expectations |
| **Complete Inventory** | Integrate all report output based on a reliable key field (i.e. ‘IP Address’) to gain a complete picture of the controls implemented for each system in your environment. | ‘raw’ synthesized spreadsheet with one row for each system in the enterprise, tied to a key field and containing all of the unique columns from each of the tools run in the previous step |
| **Risk Analysis Process** | Extract a list of all ‘major’ systems from the synthesized spreadsheet and transpose them to the *BCF - System Risk Analysis Spreadsheet*. Choose the appropriate ‘risk’ characteristics in the ‘System Data’ tab so the system/application accurately reflects the status of those controls. | A filled-out ‘System Data’ tab in the *BCF - System Risk Analysis Spreadsheet* |
| **Process Delta Report** | We’ll be generating remediation plans in the spreadsheet above, for each system whose protection posture doesn’t align with the importance the business assigns to it. However, it may be apparent at this point in the process that there are systems within your enterprise that are either falling outside of your stated IT processes, or that your IT organization is lacking some of the more essential processes other organizations find essential.  Consider the data you gathered in ‘System Data’ tab and refer to the BCF - Process Delta Checklist. | Indicate those processes that are either undocumented, missing or not consistently followed by placing a checkmark in the ‘Followed?’ column of the worksheet. |

# **Business Impact Analysis**

This process involves three workshops with both business and technology stakeholders. The purpose of this process is to gain a macro-level view of the essential business processes for each business unit, rate their importance, and understand the relationship between business processes and their dependence on technology.

|  |  |  |  |
| --- | --- | --- | --- |
| **Process Name** | **Description** | **Participants** | **Time** |
| **Major Business Process (MBP) to BU mapping** | Identify essential business processes for each business unit (BU) and quantify those processes that are centralized for the entire organization.  Determine Maximum Tolerable Downtime (MTD) for each business process. | Stakeholders who can speak authoritatively on the following topics:   * Business Processes at the BU level (perhaps one representative per BU?) * Business processes at the centralized organization level * IT representatives that can help focus on those business processes with technology dependencies | Estimated: 2.5 hours |
| **Process to Technology (P2T) Mapping - Workshop** | Map business processes to key underlying technology components.  Determine Recovery Time Objective (RTO) for each | Stakeholders who can speak authoritatively on the following topics:   * Business process function and which technologies matter most for the process to deliver required functionality * IT representatives assist mapping the business process to specific technologies and answer questions about which components are essential | Estimated: 2.75 hours |
| **Technology RPO and Component Mapping Workshop** | Determine the Recovery Point Objective (RPO) for each of the supporting technologies. | Stakeholders who can speak authoritatively on the following topics:   * Business process impact and specifics around how much data can be recovered and addressed by non-technical means. * IT representatives assist mapping the business process to specific technologies and answer questions about which components are essential | Estimated: 2.5 hours |

# **Generate System Remediation Plans**

This process will take care of itself when the *BCF - System Risk Analysis Spreadsheet is completed.* Once the ‘System Data’ tab is complete, and the ‘Tier Values’ tab is updated from our discussions with the business, then you can load and run the macro ‘BCF - System Risk Analysis Spreadsheet.vba’ and it will populate the remediation activities tabs (RemPlan-n) based on the values in the aforementioned tabs.

# **Generate System Validation Plans**

Validation plans will probably vary widely by company, but they will essentially boil down to a handful of similar activities that include:

1. Generating help desk tickets or change orders based on the output of the remediation plan spreadsheet output
2. Prioritizing activities based on the tier of the resource involved
3. Identify initial recovery targets for a backup recovery and validation ‘test run’ to measure the difference between actual recovery and validation time against RTO and RPO requirements.
4. Create a project plan for exercising Tier 1-3 systems over the next (n) years that is commensurate with the business’ expectations for reliability and accountability. Focus on reducing the effort to include representative systems, for instance, recovery of systems in a particular public or private cloud that share similar characteristics with a number of other systems in that same target environment.
5. Adjust the ‘Business Continuity Validation Calendar’ to map out recovery activities for key systems throughout the year. Centralize the recovery benchmarks and validation activities and update the risk report with information that reflects each system's ability to comply with RTO and RPO values.

# **Generate Business Continuity Plan**

Using the Business Continuity Plan template document, update it with the following information:  
  
Appendix A: Contact List

Appendix C – Major Business Process to BU Map

Appendix D – Business Process to Technology Map

Appendix E – Technology RTO

Obviously, you are welcome to make any change you like. If this document looks too large for your business purposes, contact us directly and we’ll share a smaller, more concise format we have designed.