

University of Chicago Biological Sciences Division

Cyber Security Assessment Tool (CSAT)

Cybersecurity Framework Based Assessment Tool

1 Introduction 2

2 Framework Overview 2

2.1 Framework Core 2

2.1.1 BSD CSAT Domains 4

2.2 Framework Implementation Tiers 4

2.3 Framework Profiles 4

3 BSD Cyber Security Assessment Tool (CSAT) Workbook 5

3.1 BSD Survey Department Information 5

3.2 BSD CSAT Surveys 6

3.2.1 Process Survey Options 7

3.2.2 Technology Survey Options 8

3.2.3 People Survey Options 8

# Introduction

This user guide provides an overview for utilizing the University of Chicago – Biological Sciences Division (BSD) Cyber Security Assessment Tool (CSAT). The BSD CSAT is an MS Excel based survey tool used to measure the cybersecurity capabilities of BSD departments. The tool includes two sections. The first section is the CSAT Survey. The CSAT survey section is used by BSD departments to complete the survey and is further described below. The second section is the CSAT Charts. The CSAT Charts provides reports and metrics based on survey responses from the BSD departments.

The BSD CSAT is based on the “Framework for Improving Critical Infrastructure Cybersecurity” (“the Cybersecurity Framework[[1]](#footnote-1)”). The survey questions and their corresponding results leverage the Framework Core to ensure all aspects of the cybersecurity program are assessed. The BSD CSAT expands on the Cybersecurity Framework by dividing the Framework Core categories into three (3) domains of People, Process, and Technology.

# Framework Overview

Even with the fact that companies are continuing to increase spending on cybersecurity initiatives, data breaches continue to occur. According to the Wall Street Journal, “Global cybersecurity spending by critical infrastructure industries was expected to hit $46 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc. [[2]](#footnote-2)” Despite the boost in security spending, vulnerabilities, threats against these vulnerabilities, data breaches, and data destruction persists. To combat these issues, the President on February 12, 2013 issued Executive Order (EO) 13636[[3]](#footnote-3), “Improving Critical Infrastructure Cybersecurity.” The EO directed NIST, in cooperation with the private sector, to develop and issue a voluntary, risk-based Cybersecurity Framework that would provide U.S. critical infrastructure organizations with a set of industry standards and best practices to help manage cybersecurity risks”. In February 2014, through a series of workshops held throughout the country and with industry input, NIST released the Cybersecurity Framework.

The Cybersecurity Framework, for the first time, provides a common language for communicating cybersecurity risk management at all levels in an organization and guidance that is applicable to organizations of all sizes. The Cybersecurity Framework is a risk-based approach containing three primary components: The Core, Implementation Tiers, and Framework Profiles.

## Framework Core

The Framework Core (“Core”) is a set of cybersecurity outcomes and applicable references established through five concurrent and continuous functions — Identify, Protect, Detect, Respond and Recover —that provide a strategic view of the lifecycle of an organization’s management of cybersecurity risk. Each of the Core Functions is further divided into Categories and Subcategories tied to programmatic needs and particular outcomes. The subcategories within the Framework Core identify expected outcomes for organizations to achieve when improving or developing a cybersecurity program. The subcategories provide an example of ‘what’ needs to be done, but it does not provide guidance on how an organization can achieve the outcome. Organizations can choose to obtain the outcome through a risk informed process that aligns to their organizational capabilities. The subcategories are aligned to informative references, which are a set of specific controls within proven standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each subcategory.

The BSD CSAT uses the Framework Core categories to align and track the survey questions and responses. The 22 categories defined in the Framework Core provide a comprehensive overview of key components for any cybersecurity program. Therefore, aligning the survey questions to the categories ensures all aspects of the department’s cybersecurity program is reviewed.

The BSD CSAT tool categories were adjusted for clarity within BSD. The category names, where appropriate, were revised to ensure the title of the category conveyed the subject of the category. Table 1 provides identifies the BSD CSAT Category titles used throughout the tool and their mapping to the original Framework Core categories. The BSD CSAT Category names that were realigned for clarity are shaded in red. In addition to the BSD CSAT category titles, the BSD CSAT leverages unique identifiers for each category. The identifiers are shown below and are used throughout the CSAT to easily reference the Framework Core functions and categories. The BSD CSAT identifies were derived using the identifiers established in the Framework Core as released by NIST.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **Framework Category** | **BSD CSAT Category** | **Identifier** |
| **IDENTIFY (ID)** | Asset Management | Asset Management | ID.AM |
| Business Environment | Business Environment | ID.BE |
| Governance | Governance | ID.GV |
| Risk Assessment | Risk Assessment | ID.RA |
| Risk Management Strategy | Risk Management Strategy | ID.RM |
| **PROTECT (PR)** | Access Control | Access Control | PR.AC |
| Awareness and Training | Awareness and Training | PR.AT |
| Data Security | Data Security | PR.DS |
| Information Protection Processes and Procedures | Information Protection Processes | PR.IP |
| Maintenance | Maintenance | PR.MA |
| Protective Technology | Protective Technology | PR.PT |
| **DETECT (DE)** | Anomalies and Events | Anomalies and Events | DE.AE |
| Security Continuous Monitoring | Security Continuous Monitoring | DE.CM |
| Detection Processes | Detection Processes | DE.DP |
| RESPOND (RS) | Response Planning | Response Planning | RS.RP |
| Communications | Response Communications | RS.CO |
| Analysis | Incident Analysis | RS.AN |
| Mitigation | Incident Mitigation | RS.MI |
| Improvements | Incident Review | RS.IM |
| **RECOVER (RC)** | Recovery Planning | Recovery Planning | RC.RP |
| Improvements | Recovery Improvements | RC.IM |
| Communications | Recovery Communications | RC.CO |

Table 1. Framework Core category to BSD CSAT Category mapping

### BSD CSAT Domains

While not a component of the Cybersecurity Framework, the BSD CSAT tool assesses the People, Process, and Technologies or domains within the BSD department’s cybersecurity program. Survey questions for the People domain determine the department’s ability to assign staff cybersecurity responsibilities commensurate with their skills. The Process domain assesses the defined and implemented cybersecurity capabilities within the department. The Technology domain determines if the appropriate technical capabilities are available to support the department. Leveraging the domain triad ensures the three key functions that can enable the department to provide cybersecurity services are measured.

## Framework Implementation Tiers

The Framework Implementation Tiers (“Tiers”) describe the level of sophistication and rigor an organization employs in applying its cybersecurity practices, and provides a context for applying the core functions. The Implementation Tiers explain ‘how’ an organization can achieve the outcomes provided in the Framework Core. Comprising four levels from “Partial” (Tier 1) to “Adaptive” (Tier 4), the tiers describe approaches to cybersecurity risk management that range “from informal, reactive responses to agile and risk-informed."

BSD is currently operating at Tier 2 with a target state at Tier 3. The BSD CSAT survey questions were developed with this understanding; however the Tiers are not directly tied to any questions within the tool. As departments within BSD cybersecurity programs mature, the progress from Tier 2 to Tier 3 can be inferred, but not specifically tracked.

## Framework Profiles

The Framework Profile (“Profile”) is a tool that provides organizations a method for storing information regarding their cybersecurity program. A profile allows organizations to clearly articulate the goals of their cybersecurity program. The Framework is risk-based; therefore, the controls and how they are implemented change as the risk to the organization changes. The Framework identifies two types of profiles, Current state and Target state. The current state profile describes the current organizational policy and practices for each outcome described in the Framework Core. The Target state profile provides organizations the ability to self-identify a target state for their cybersecurity program that is aligned to risk appetite and regulatory requirements. Creation of current and target profiles can help direct organizations’ efforts toward improved cybersecurity in a methodical manner.

The BSD CSAT provides an overview of the current maturity of each BSD department completing the survey. While the survey results do not represent a full Framework Profile, the results provide enough information about the department to demonstrate how the departments implementing cybersecurity controls and therefore may be considered a rudimentary Framework Profile.

# BSD Cyber Security Assessment Tool (CSAT) Workbook

The CSAT is an MS Excel based workbook that presents survey questions and records the results of the question. The CSAT is divided into several tabbed worksheets. The worksheets include: Instructions, Department Info, Process, Technology, People, Dashboard, and Radar Chart. Table 2 provides a description for each of the tabs within the CSAT workbook.

| Tab | Description |
| --- | --- |
| Instructions | Provides an overview of each of the remaining tabs within the workbook. |
| Department Info | Records information regarding the department completing the survey including: department name, section name, the date the survey was completed, and the contact information of the survey taker and key points of contact. Because scoring is often subjective, staff may need to be contacted for additional clarification. |
| People | Contains customized survey questions specifically related to the departments personnel resource capability, availability and accountability. Rating definitions for survey responses to People questions are provided in the legend at the top of this tab. |
| Process | Contains customized survey questions specifically related to the nature of the departments processes and their execution. Rating definitions for survey responses to Process questions are provided in the legend at the top of the Process tab. |
| Technology | Contains customized survey questions related to the departments technology resources and their sufficiency. Rating definitions for survey responses to Technology questions are provided in the legend at the top of the Technology tab. |
| Dashboard | Provides a summary of the departments’ cybersecurity capabilities. This tab is initially blank until the survey is complete. Once the survey is complete this tab graphically depicts the implementation status of the department’s cybersecurity program. |
| Radar Chart | Tracks survey metrics as they are completed as well as identifying outstanding questions that remain to be completed by domain (people, process, technology). The graphic representation also overlays the department status against the BSD Target State profile for easy comparison. |

Table 2. BSD Survey Workbook Tabs

## BSD Survey Department Information

Prior to completing the survey the information regarding the department completing the survey should be recorded in the Department Info tab. To fill out the department information, simply select the Department Info tab and enter the information regarding the department. Table 3 provides a summary of the information collected within this tab. The data entry in this tab is not validated and accepts free form text.

| Title | Description |
| --- | --- |
| Department Name | Records the name of the department completing the survey |
| Section Name | If a subsection within the department is completing the survey, enter the sections name in this field. |
| Date Complete | The date the survey was completed. |
| Survey Point Person | This is the single point within the department responsible for ensuring the survey is complete. The BSD ISO will contact this individual if there are any questions arising from the survey’s results. |
| Point Person Email | The email address for the survey point person. |
| Point Person Phone # | The phone number of the survey point person. |
| EA Name | The Executive Administrator (EA) of the department at the time the survey was completed. |
| EA Email | The email address for the EA. |
| IT Contact Name | The IT Manager assigned to the department at the time of the survey. In many cases this may be the same person as the survey point person |
| IT Contact Email | The IT Managers email address |
| Name of Survey Contributors | Record the names of anyone contributing the responses within the survey. This information is maintained for historical purposes only. |

Table 3. Dashboard Tab Data Points

## BSD CSAT Surveys

As previously stated the survey questions are divided into three domains: Process, Technology, and People. Each domain has a separate tab within the CSAT Survey section. To complete the survey simply select the tab of the corresponding domain you wish to complete. Once selected the response options are provided at the top of the sheet for easy reference. Table 4 provides an overview of the information provided with each survey question.

| Title | Description |
| --- | --- |
| Question ID | A unique identifier to track survey questions and their associated responses. The question ID includes the Function, Category and Domain separated by a period. The number indicates how many questions are linked to the function, category and domain pairing. It is important to note that the question IDs are reused between surveys. Therefore, if a question is updated in a future survey the same question ID will be reused. |
| Function | The Framework Core Function being assessed by the survey q |
| Question | The survey question itself. The survey questions are high-level questions assessing different components of the department’s cybersecurity program. |
| Response | A pull down menu available to the survey responder for selecting the most appropriate response to the question. All survey questions must be answered. Individuals completing the survey should select the most appropriate or best answer based on their understanding of the department’s capabilities. |
| Additional Info | Provides additionally information regarding the survey question. This information is not intended to influence the person completing the survey. Rather, it provides additional context to facilitate the selection of the most appropriate response. |
| Notes | A free form text field for the individual(s) completing the survey to record comments associated to their survey results. The notes do not influence the summary rating provided by the BSD CSAT; however, the notes may be used |

Table 4. Survey Question Data Points

When completing the survey questions select the best possible answer. In some cases you may find that two or more options are appropriate. Using your best judgment select the most appropriate answer and provide a note in the Notes column explaining your rationale for selecting the indicated response. All survey questions must be answered except for those that appear in grey cells. The grey cells denote questions that are only applicable at a BSD level. The ratings for these questions should be predetermined and hardcoded into the DataSheet\_Hide administrative tab. If none of the available responses are appropriate for a given survey question select the most appropriate answer and provide your rationale for your selection in the Notes column.

### Process Survey Options

Each domain provides a standard set of responses for answering survey questions in that domain. Table 5 provides a summary of the Process response options and their description.

| Title | Description |
| --- | --- |
| No Process | - The tasks associated with this activity are not performed. |
| Ad-Hoc | - There is no documentation associated with the activity. - The tasks associated with this activity are performed in an ad-hoc manner. |
| Defined | - Some written documentation exists for addressing the activity - the documentation is only partially implemented or followed in practice. |
| Repeatable | - Appropriate documentation exists for addressing the activity. - The activity is mostly performed in accordance with the documentation. |
| Formal | - Appropriate documentation exists for addressing the activity and aligns with BSD policy and standards. - the activity is performed in accordance with BSD policy and standards |

Table 5. Process Survey Response Options

If Formal is selected as the most appropriate response option, supporting artifacts (e.g. process and procedures) must be provided to BSD ISO.

### Technology Survey Options

Each domain provides a standard set of responses for answering survey questions in that domain. Table 6 provides a summary of the Technology response options and their description.

| Title | Description |
| --- | --- |
| Inadequate | - The appropriate technology required to perform this activity is not available within the department. |
| Lacking | - The primary intent of the technology being used to complete the activity is not the intended purpose. |
| Adequate | - The technology is capable and configured to perform some of the required activities - There is limited infrastructure, computing power, or software licenses available to the department for performing the required activity. |
| Sufficient | - The technology is capable and configured to perform most of the required activity. - There is enough infrastructure, computing power, and software licenses available to the department for performing the required activity. |
| Optimal | - The activity is able to be completed in its entirety with the technology. - The primary function of the technology is to perform the required activity. - There is ample infrastructure, computing power, and software licenses available to the department for performing the required activity. |

Table 6. Technology Survey Response Options

If Optimal is selected as the most appropriate response option, supporting artifacts (e.g. technology names, number of licenses available, etc) must be provided to BSD ISO.

### People Survey Options

Each domain provides a standard set of responses for answering survey questions in that domain. Table 7 provides a summary of the Technology response options and their description.

| Title | Description |
| --- | --- |
| Inadequate | - The activity is not able to be performed due to staff having limited skill set. - The activity is not able to be performed due to lack of staff availability. - No staff is responsible for completing the activity. |
| Lacking | - The current staff have limited skills that only enable them to perform a small portion of the activities - The staff perform the activities as they have availability, but it is resource intensive and detracts from other responsibilities |
| Adequate | - The current staff have the skills to perform most responsibilities associated with the activity - The staff perform the activities as they have availability, but it is resource intensive and detracts from other responsibilities. |
| Informal | - Most responsibilities associated with the activity are able to be performed with the current quantity of staff and knowledge base without significant burden. - The staff are accountable for performing the activity without being formally assigned. |
| Formal | - The staff has sufficient skills and experience to complete the activity its entirety with little burden. - Staff has been explicitly designated roles and responsibilities for completing the activity. |

Table 7. People Survey Response Options

If Formal is selected as the most appropriate response option, supporting artifacts (e.g. appointment letters, role descriptions, etc) must be provided to BSD ISO.

1. The National Institute of Technology and Standards (NIST) “Framework for Improving Critical Infrastructure Cybersecurity version 1.0”, February 12, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> [↑](#footnote-ref-1)
2. *Companies Wrestle With the Cost of Cybersecurity*, February 25, 2014, http://online.wsj.com/news/articles/SB10001424052702304834704579403421539734550 [↑](#footnote-ref-2)
3. Executive Order 13636 of February 12, 2013, *Improving critical Infrastructure Cybersecurity*, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [↑](#footnote-ref-3)