SABSA®

Release 1.0

The SABSA Institute™

SENC Project Team TSI

Glen Bruce – Project Lead

Maurice Smit – deputy Chief Architect TSI

March 2023

[redacted]

## Trademarks

SABSA® is a registered trademark of The SABSA Institute. Other trademarks owned by The SABSA Institute are labelled with a TM mark on their first occurrence in the text.

All other brand, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

# TABLE OF CONTENTS

# 1 The SABSA Institute Recommendations for the NIST CSF Framework 2.0

The SABSA Institute (TSI) is a not-for-profit organisation that governs the integrity and future development of SABSA intellectual property and provides member services to the international SABSA community. TSI is incorporated as a Community Interest Company in the UK, subject to the governance rules for C.I.C.s, but it's sphere of activity is global, with more than 7,000 certified SABSA security architects in more than 50 countries.

SABSA® is a methodology for developing business-driven, risk and opportunity-focused enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. It is an open standard, comprising several frameworks, models, methods and processes, free for use by all, with no licensing required for end-user organisations who make use of the standard in developing and implementing architectures and solutions.

The SABSA Institute (TSI) would like to take advantage of the opportunity to provide input into the next version of the NIST Cybersecurity Framework (CSF). Many organizations that have or are developing SABSA-based security architectures also use the NIST CSF. The NIST CSF has become one of the more popular security frameworks, embraced by many industries, regulatory bodies and even countries as the leading method for applying processes and controls to deal with ever-evolving cyber threats.

The SABSA Institute (TSI) is recommending additions to the NIST CSF v2 related to three (3) specific themes (Themes #4, #5 and #6) outlined in the NIST CSF V2 Concept Paper.

## 1.1 The New Govern Function

Effective governance breaks down barriers across the organization and collectively manages organizational and business risk to drive efficient delivery of business value. The initial planning for the NIST CSF included a management function in addition to the other five functions (Identify, Protect, Detect, Respond and Recover). The management function was intended to apply across the other five functions but was dropped before the NIST CSF was first published. The addition of a Govern Function will rectify this important omission. An initial consideration is how to illustrate the Govern Function in relation to the other five. One of the more obvious solutions would be to place the Govern Function in the middle of the diagram to illustrate how it spans across all the other five functions.

We recommend the Governance Function include the categories as illustrated in Figure 1. This figure provides a high-level illustration of the recommended categories for the new Govern Function. The light green shaded boxes illustrate new recommended categories.

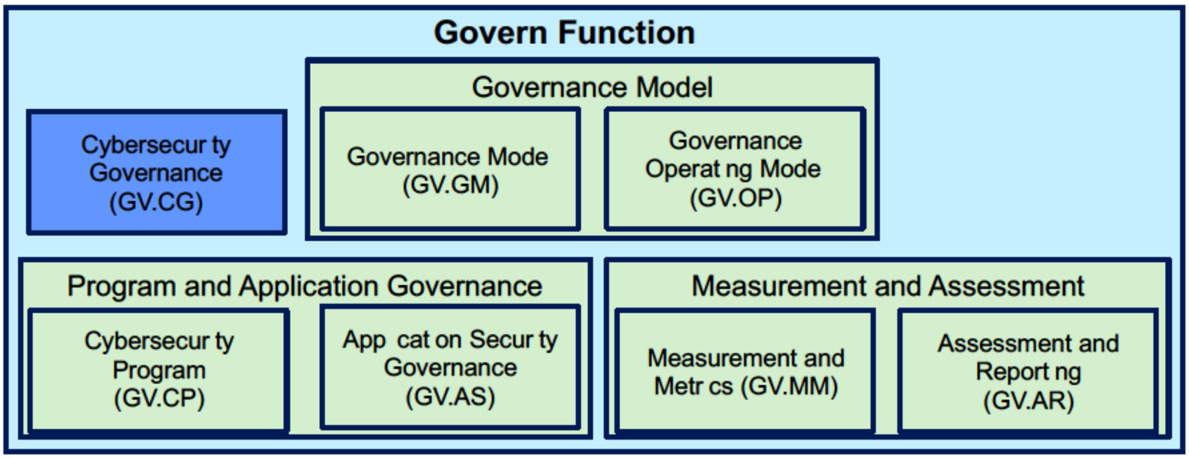
Govern Function
Governance Model
Cybersecurity Governance (GV.CG)
Governance Model (GV.GM)
Governance Operating Model (GV.OP)
Program and Application Governance
Measurement and Assessment
Cybersecurity Program (GV.CP)
Application Security Governance (GV.AS)
Measurement and Metrics (GV.MM)
Assessment and Reporting (GV.AR)

*Figure 1. Organization of proposed new categories for the NIST CSF 2.0 Govern Function*

The following are specific recommendations for the new Govern Function, including additional categories and sub-categories in support of this new function.

### 1.1.1 Modify the existing Governance Category

1. Identify the new Govern Function with the label (GV).
2. Relabel the existing Governance category (ID.GV) to the Cybersecurity Governance category (GV.CG) and place it under the new Govern Function (GV).

   The existing Governance category should be relabelled to Cybersecurity Governance (GV.CG) to avoid any confusion with the Governance category under the existing Identify Function. The sub-categories under the existing Governance category should be "shifted" to fall under the Cybersecurity Governance (GV.CG) category and be relabelled accordingly.

3. List sub-categories that are currently identified under the Governance category (ID-GV) under the Cybersecurity Governance category (GV-CG) and relabel from ID.GV-1, ID.GV-2, ID.GV-3 and ID.GV-4 to GV-CG-1, GV.CG-2, GV.CG-3 and GV.CG-4.
4. Under the renamed Cybersecurity Governance category (GV.CG) for the establishment and management of overall cybersecurity governance include the following new sub-categories:
   a) Clear and concise definitions and a taxonomy for cybersecurity governance terms and functions are identified (GV.CG-5).
   b) The relationship between the business context of the organization and the security context of the operational cybersecurity program is identified and documented (GV.CG-6).
   c) The responsibilities for audits, auditing and continuous assurance activities include the definition of who is responsible to conduct, manage and communicate the results of audit and assurance activities (GV.CG-7).
   d) Cyberattacks and detected reconnaissance activities are disclosed to national and/or international security agencies or regulatory bodies as required (GV.CG-8).

### 1.1.2 Recommended Governance Model Categories

1. Create a Governance Model Category (GV.GM) to include the sub-categories related to the defining, implementing and operation of the overall governance model for cybersecurity governance.

Cybersecurity Governance must be subject to an ongoing management process to ensure the governance components are known, relevant and providing the intended guidance directing the organization's responsibility for various aspects of the Information Security Governance Process is allocated to several bodies within the organization.

The identification of the organization's decisions on management of risk in relation to the business and the specification of the roles, responsibilities and processes required to carry out those risk decisions are defined, implemented and managed on a continual basis (GV.GM.

2. Include the following new sub-categories under the Governance Model (GV.GM) category:

   a) The authority for cybersecurity is identified, assigned, and integrated into overall corporate governance (GV.GM-1).
   b) The responsibility for integration/alignment with enterprise risk management is assigned and implemented (GV.GM-2).
   c) The defined governance model includes continuous assurance of the effectiveness of the information security program as well as the design and operational effectiveness of the supporting processes and practices (GV.GM-3).
   d) The governance model is defined and implemented through a detailed and documented operating model (GV.GM-4).
   e) There are defined requirements for the levels of governance including continuous monitoring and oversight of operational function, evaluation of the results against business requirements, and directing remediation and process improvements where required (GV.GM-5).

3. Add a new category called the Governance Operating Model (GV.OP) to include the sub-categories required to operate cybersecurity governance on an ongoing basis.

   The specification and implementation of required operating components for implementing, maintaining, and managing the governance model are implemented to provide effective oversight and management of cybersecurity risks (GV.OP).

4. Add new sub-categories to the Governance Operating Model category (GV.OP) to include the sub-categories that manage governance processes.

   a) A defined cybersecurity policy framework including the hierarchy of security decisions is reflected in the principles, policies, directives, procedures, and standards that have been defined and implemented to support the policy/standards lifecycle (GV.OP-1).
   b) Active enforcement of compliance to the cybersecurity policies and standards is conducted on a regular basis (GV.OP-2).
   c) There are traceable links from the organization's business objectives to cybersecurity decisions and implemented solutions (GV-OP-3).
   d) There is defined and effective communication across all levels of the organization concerning the effective operation and status of cybersecurity to continuously assure and elevate the organization's culture for effective information protection and security (GV-OP-4).

### 1.1.3 Recommended Cybersecurity Program Governance and Application Security Governance Categories

We recommend two additional categories for the Govern Function (GV), Cybersecurity Program Governance (GV.CP) and Application Security Governance (GV.AS).

1. Create a new Cybersecurity Program category (GV.CP) to provide direction on the establishment, operation, and ongoing management of all the high-level requirements for operating the organization's cybersecurity program.

   The overarching collection of the cybersecurity responsibilities, decisions, strategies, architectures, reference documents, principles, policies, processes, and procedures have been defined, implemented, and operated as the cybersecurity program (GV.CP).

2. Add new Cybersecurity Program sub-categories related to the development, operation, and management under the Cybersecurity Program (GV.CP) category.

   a) The accountable sponsor for the Enterprise Cybersecurity Program is identified and is provisioned with the appropriate authority and resources (GV.CP-1).
   b) The strategy, goals, objectives and key outcomes for the cybersecurity program are defined, documented and used to anchor the program (GV.CP-2).
   c) The cybersecurity program is subject to periodic plan updates and independent assurance reviews (GV.CP-3).
   d) An enduring cyber security requirements management capability has been used to define, measure and track security requirements throughout the entire life of projects (GV.CP-4).
   e) Enterprise-wide knowledge management capabilities for cybersecurity are known and available. (GV.CP-5).

3. Include an Application Security Governance category (GV.AS) to include specification for governance of internally developed applications.

   Any applications that are developed in-house must be developed and delivered under strict control to minimize the introduction of vulnerabilities or potential threats to the environment.

   Applications that are developed and delivered in-house are based on defined security criteria and under strict development control to prevent vulnerabilities and reduce potential threats from being introduced into the environment (GV.AS).

4. Add Application Governance sub-categories identifying specific criteria to be used to reduce the risk of threats or compromise when applications are designed, developed, and delivered.

   a) To address cybersecurity risks, a risk-based secure software development policy is used to guide the internal development of applications. (GV.AS-1).
   b) Threat modelling is completed and maintained for the whole life of all applications that are internally developed (GV.AS-2).
   c) Risk-based Secure software development standards and practices are applied, and formal testing is conducted for all applications that are internally developed (GV.AS-3).
   d) Software verification and validation activities are enforced to the organization's specifications for applications that are internally developed. This includes adding cybersecurity testing activities to existing software testing activities (GV.AS-4).

## 1.2 Recommended Measurement and Assessment Categories

In support of theme #4—"CSF 2.0 will advance understanding of cybersecurity **measurement and assessment**"—the NIST CSF 2.0 would benefit from providing guidance for measurement, metrics, assessment and reporting through additional categories and sub-categories. Since measurement and assessment should span all functions, we recommend two additional categories for the new Govern function.

### 1.2.1 Measurement and Metrics Category

It is important to understand the operation and effectiveness of the processes and controls that are used to deliver the various NIST CSF sub-categories. This requires the collection and analysis of measures and supporting metrics to derive information on the execution and effectiveness of the sub-categories. Thresholds can be applied to the measures and the metrics to provide relative indicators of operation. For selected measures and metrics, thresholds can be applied using risk levels to provide an indication of relative risk. The collection of measures and metrics may be further used to create key indicators (risk and/or performance) that provide further insight into the operation of the categories and can be summarized to indicate the relative success of the operation of the categories and functions. The operation and effectiveness of the sub-categories and categories provides insight into the relative management of risk beyond the simple presence or absence of controls and processes. In addition, including the metrics and requirements from a Business Impact Analysis as found in NIST 800-34 Rev, 1 provides context as to the business requirements and prioritization.

1. Include a new Measurement and Metrics (GV.MM) category to specify the requirements for measuring and providing metrics for the operation and management of the cybersecurity program.

   The requirements for measuring and providing metrics for the operation and management of the cybersecurity program in relation to the organization's business context and risk are defined and implemented to indicate the current effectiveness of the Cybersecurity Program (GV.MM)

2. Define additional sub-categories to specify the requirements for measures, measurements, and metrics across all CSF functions. We recommend the following sub-categories under the GC-MM category:

   a) Reference to a common and consistent set of definitions and taxonomy is provided for measures, measurements, metrics, etc. and specified in the current version of NIST 800-55 Performance Measurement Guide for Information Security. Definitions are positioned in the context of cybersecurity (GV.MM-1).
   b) Measures are specified at each process and/or control level that supports individual sub-categories across the NIST CSF where available (GV.MM-2).
   c) Key reporting measures and metrics are defined for each sub-category where appropriate for the organization (GV.MM-3).
   d) The most appropriate measurement approach for the metrics program is determined (e.g., Risk Heat Map for less mature organisations up to quantitative risk measurement for higher maturity organisations) (GV.MM-4).
   e) Measures and metrics are defined at the process level as well as the control level for all categories (GV.MM-5).
   f) Methods are in place to measure the effectiveness of the operating processes and controls, not just the presence and depth of definition and implementation (GV.MM-6).

### 1.2.2 Assessment and Reporting Category

In many organizations, the NIST CSF is regularly used as the reference standard for assessing the relative maturity of a cybersecurity program, usually leveraging the CMMI maturity levels. This is an area that would benefit from additional guidance to provide a wider industry-related view for broader comparisons. We recommend using an approach to define relative maturity level criteria, using the six (levels 0-5) CMMI levels, similar to the approach used for the Cybersecurity Maturity Model Certification (CMMC) program. It would also be very beneficial to describe the differing maturity level criteria to the NIST CSF practices and processes in a similar manner as the CMMC maturity guidance. It is important to include considerations for assessing the effectiveness of the operation of the controls and processes to arrive at an accurate maturity level not just the specification and existence of the controls and processes.

1. Create an Assessment and Reporting category (GV.AR) related to the NIST CSF assessment method, and reporting requirements on the design, operation and effectiveness of the cybersecurity program. Placement of this category under the Govern Function demonstrates the applicability of the sub-categories is across all NISR CSF functions.

   The definition of requirements, specifications, operation, and management of NIST CSF assessment methods and reporting requirements on the design, operation, and effectiveness of the cybersecurity program are defined, implemented and operate on an ongoing basis to report on the effectiveness of the Cybersecurity Program (GV.AR).

2. Include the following new sub-categories:

   a) A common and consistent method for assessing and assigning maturity levels to allow cross organization or industry comparisons is in place (GV.AR-1).
   b) A business impact analysis (BIA) identifying and prioritizing information systems and components and assessing criticality of assets and the risks to those business assets or systems in relation to identified key assets of the organization has been completed to guide the required protections (GV.AR-2).
   c) There is a defined relationship between the measures and metrics for implemented controls and processes, including risk thresholds that have been applied to the measures and metrics to aid assessing the effectiveness of the controls and processes (GV.AR-3).
   d) A method has been implemented to aggregate both assessed maturity levels and resulting risk levels to arrive at an overall maturity level reflecting the risk to the organization when formally assessed (GV.AR-4).
   e) Assigned management responsibilities to provide assurance for senior management include conducting periodic, independent reviews or assessments of the cybersecurity security program (GV.AR-5).

## 1.3 Cybersecurity Supply Chain Risk Management (C-SCRM) Category Recommendations

The increasing complexities that arise from delivering business through a mix of suppliers, service providers and business partners heighten cybersecurity risks. We recommend adding a few sub-categories to the existing Supply Chain Risk Management (ID.SC) category to address this reality. We also recommend that product suppliers, including product support, service providers and business partners, be classified as supply chain participants. It is important to consider all components of the business partners, supply chain and service providers, including those organizations that the partners, suppliers and providers rely on, and can impact their ability to deliver to your organization.

### 1.3.1 Specific Recommendations for Cybersecurity and Supply Chain Risk Management (C-SCRM)

1. Add the following sub-categories to the existing Supply Chain Risk Management category (ID.SC). enhancement to include C-SCRM requirements more fully in the NIST CSF:

   a) Supply chain dependencies and ongoing surveillance of these dependencies is understood and documented to manage potential risks (ID.SC-6).

b) Requirements are defined for important security-related vendor relationships, including vetting and ongoing management (ID.SC-7).
c) Criteria are defined for assessment of business partner, service provider and supplier security requirements in relation to the levels required by the business, permitting extension of these business relationships into business partners’ operations in a trusted manner (ID.SC-8).
d) Defined security criteria and service level agreements are in place and used to manage security requirements between the organization and business partners, suppliers and service providers ID-SC-9).
e) Third-party responsibilities in relation to business infrastructure are visible and managed (ID.SC-10).

# 2 Appendix: NIST CSF 2.0 Category and Sub-category Recommendations Summary

**This table contains all the recommended categories and sub-categories identified in the main section. Many of the categories and sub-categories are for the new Govern function. The sub-categories that are shaded in grey indicate existing sub-categories in the current version 1.1 of the NIST CSF.**

| Function | Category | Sub-category |
|---|---|---|
| | **Cybersecurity Governance (GV.CG):**<br>The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | **GV.CG-1:** Organizational cybersecurity policy is established and communicated. |
| | | **GV.CG-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. |
| | | **GV.CG-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood, and managed. |
| | | **GV.CG-4:** Governance and risk management processes address cybersecurity risks. |
| | | **GV.CG-5:** Clear and concise definitions and a taxonomy for cybersecurity governance terms and functions are identified. |
| | | **GV.CG-6:** The relationship between the business context of the organization and the security context of the operational cybersecurity program is defined and documented. |
| | | **GV.CG-7:** The responsibilities for audits, auditing and continuous assurance activities include the definition of who is responsible to conduct, manage and communicate the results of audit and assurance activities. |
| | | **GV.CG-8:** Cyberattacks and detected reconnaissance activities are disclosed to national and/or international security agencies or regulatory bodies as required. |
| | **Governance Model (GV.GM):**<br>The identification of the organization's decisions on management of risk in relation to the business and the specification of the roles, responsibilities and processes required to carry out those risk decisions are defined, implemented and managed on a continual basis. | **GV.GM-1:** The authority for cybersecurity is identified, assigned and integrated into overall corporate governance. |
| | | **GV.GM-2:** The responsibility for integration/alignment with enterprise risk management is assigned and implemented. |
| | | **GV.GM-3:** The defined governance model includes continuous assurance of the effectiveness of the information security program as well as the design and operational effectiveness of the supporting processes and practices. |
| | | **GV.GM-4:** The governance model is defined and implemented through a detailed and documented operating model. |
| | | **GV.GM-5**: There are defined requirements for the levels of governance including continuous monitoring and oversight of operational function, evaluation of the results against business requirements and directing remediation and process improvements |

| Function | Category | Sub-category |
|---|---|---|
| 🟩 | | where required. |
| | **Governance Operating Model (GV.OP):** The specification and implementation of required operating components for implementing, maintaining, and managing the governance model are implemented to provide effective oversight and management of cybersecurity risks. | **GV.OP-1:** A defined cybersecurity policy framework including the hierarchy of security decisions is reflected in the principles, policies, directives, procedures, and standards that have been defined and implemented to support the policy/standards lifecycle. |
| | | **GV.OP-2:** Active enforcement of compliance to the cybersecurity policies and standards is conducted on a regular basis. |
| | | **GV.OP-3:** There are traceable links from the organization's business objectives to cybersecurity decisions and implemented solutions. |
| | | **GV.OP-4:** There is defined and effective communication across all levels of the organization concerning the effective operation and status of cybersecurity to continuously assure and elevate the organization's culture for effective information protection and security. |
| | **Cybersecurity Program (GV.CP):** The overarching collection of the cybersecurity responsibilities, decisions, strategies, architectures, reference documents, principles, policies, processes, and procedures have been defined, implemented and operated as the cybersecurity program. | **GV.CP-1:** The accountable sponsor for the Enterprise Cybersecurity Program is identified and is provisioned with the appropriate authority and resources. |
| | | **GV.CP-2:** The strategy, goals, objectives and key outcomes for the cybersecurity program are defined, documented and used to anchor the program. |
| | | **GV.CP-3:** The cybersecurity program is subject to periodic plan updates and independent assurance reviews. |
| | | **GV.CP-4:** An enduring cybersecurity requirements management capability has been used to define, measure and track security requirements throughout the entire life of projects. |
| | | **GV.CP-5:** Enterprise-wide knowledge management capabilities for cybersecurity are known and available. |
| | **Application Security Governance (GV.AS):** Applications that are developed and delivered in-house are based on defined security criteria and under strict development control to prevent vulnerabilities and reduce potential threats from being introduced into the environment. | **GV.AS-1:** To address cybersecurity risks, a risk-based secure software development policy is used to guide the internal development of applications. |
| | | **GV.AS-2:** Threat modelling is completed and maintained for the whole life of all applications that are internally developed. |
| | | **GV.AS-3:** Risk-based Secure software development standards and practices are applied, and formal testing is conducted for all applications that are internally developed. |
| | | **GV.AS-4:** Software verification and validation activities are enforced to the organization's specifications for applications that are internally developed. This |

| Function | Category | Sub-category |
|---|---|---|
| 🟩 | | includes adding cybersecurity testing activities to existing software testing activities. |
| 🟩 | **Measurement and Metrics (GV.MM)**:<br>The requirements for measuring and providing metrics for the operation and management of the cybersecurity program in relation to the organization's business context and risk are defined and implemented to indicate the current effectiveness of the Cybersecurity Program. | **GV.MM-1:** Reference to a common and consistent set of definitions and taxonomy is provided for measures, measurements, metrics, etc. and specified in the current version of NIST 800-55 Performance Measurement Guide for Information Security. Definitions are positioned in the context of cybersecurity. |
| 🟩 | | **GV.MM-2:** Measures are specified at each process and/or control level that supports individual sub-categories across the NIST CSF where available. |
| 🟩 | | **GV.MM-3:** Key reporting measures and metrics are defined for each sub-category where appropriate for the organization. |
| 🟩 | | **GV.MM-4:** The most appropriate measurement approach for the metrics program is determined (e.g., Risk Heat Map for less mature organisations up to quantitative risk measurement for higher maturity organisations). |
| 🟩 | | **GV.MM-5:** Measures and metrics are defined at the process level as well as the control level for all categories. |
| 🟩 | | **GV.MM-6:** Methods are in place to measure the effectiveness of the operating processes and controls, not just the presence and depth of definition and implementation. |
| 🟩 | **Assessment and Reporting (GV.AR)**:<br>The definition of requirements, specifications, operation, and management of NIST CSF assessment methods and reporting requirements on the design, operation, and effectiveness of the cybersecurity program are defined, implemented and operate on an ongoing basis to report on the effectiveness of the Cybersecurity Program. | **GV.AR-1:** A common and consistent method for assessing and assigning maturity levels to allow cross organization or industry comparisons is in place. |
| 🟩 | | **GV.AR-2:** A business impact analysis (BIA) identifying and prioritizing information systems and components and assessing criticality of assets and the risks to those business assets or systems in relation to identified key assets of the organization has been completed to guide the required protections. |
| 🟩 | | **GV.AR-3:** There is a defined relationship between the measures and metrics for the implemented controls and processes, including risk thresholds that have been applied to the measures and metrics to aid assessing the effectiveness of the controls and processes. |
| 🟩 | | **GV.AR-4:** A method has been implemented to aggregate both assessed maturity levels and resulting risk levels to arrive at an overall maturity level reflecting the risk to the organization when formally assessed. |
| 🟩 | | **GV.AR-5:** Assigned management responsibilities include conducting a periodic, independent review or assessment on the cybersecurity security program. |
| 🟦 | | **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders |

| Function | Category | Sub-category |
|---|---|---|
| **Identity**<br>**(ID)** | **Supply Chain Risk Management (ID.SC):**<br>The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks. | **ID.SC-2:** Identify, prioritize, and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process |
| | | **ID.SC-3:** Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan. |
| | | **ID.SC-4:** Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted |
| | | **ID.SC-5:** Response and recovery planning and testing are conducted with critical suppliers/providers |
| | | **ID.SC-6:** Supply chain dependencies and ongoing surveillance of these dependencies is understood and documented to manage potential risks. |
| | | **ID.SC-7:** Requirements are defined for important security-related vendor relationships, including vetting and ongoing management. |
| | | **ID.SC-8:** Criteria are defined for assessment of business partner, service provider and supplier security requirements in relation to the levels required by the business, permitting extension of these business relationships into business partners' operations in a trusted manner. |
| | | **ID.SC-9:** Defined security criteria and service level agreements are in place and used to manage the security requirements between the organization and business partners, suppliers and service providers. |
| | | **ID.SC-10:** Third-party responsibilities in relation to business infrastructure are visible and managed. |

*Table 1. Recommended categories and sub-categories for NIST CSF V2*