#### 4.1 Identify Function.

The Identify Function is foundational to the risk assessment process. It is highly recommended that risk management practitioners start with the Identify Function. Consideration of the organization’s mission and business objectives, threat environment, assets, and vulnerabilities will have a significant influence on the overall risk and will directly impact the other four CSF Functions (i.e., Protect, Detect, Respond, Recover).

The objectives of the Identify Function include:

* Identify the business or operational environment and organization’s purpose.
* Identify all assets, including hardware, software and personnel.
* Identify sources and infrastructure that provide SOC functionality; and
* Identify the vulnerabilities, threats, and impacts should the threat be realized in order to assess the risk.

The Identify Function within the Cybersecurity Framework defines six Categories, five of which have at least one Subcategory that applies to SOC to varying degrees, as summarized in Sections 4.1.1 through 4.1.5.

##### 4.1.1 Asset Management Category

The data, personnel, devices, systems, and facilities that enable the organization to achieve its business objectives are identified and managed in a manner that is consistent with their importance to organizational objectives and the organization’s risk strategy.

There are six Subcategories within Asset Management, four of which apply to the SOC.

| Identify: Asset Management Category |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.AM-1: Physical devices and systems within the organization are inventoried. | Document and maintain an inventory of the components that reflect the current system. Consider incorporating a configuration management tool that documents the physical location of all physical components and verify with physical inspections. During physical inspections, identify equipment and its physical interfaces.  | **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2.3 |
| ID.AM-2: Software platforms and applications within the organization are inventoried. | Document and maintain an inventory of software components, such as software license information, software version numbers for applications, software, and operating systems. System software inventory is reviewed and updated as defined by the organization. | **NIST SP 800-53 Rev. 5** CM-8, PM-5 |
| ID.AM-3: Organizational communication and data flows are mapped. | Identify all connections within and between the systems. All connections and interfaces are documented, authorized, and reviewed.Connection information may include the physical interface characteristics, logical interface characteristics, data characteristics, ports, protocols, addresses, security requirements, and nature of the connection. | **NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8, SA-17**IEC 61850-90-4** 10, 14 |
| ID.AM-4: External information systems are catalogued | There may be different organizations commanding the bus and the payload, however a command to the payload will be encrypted and tunneled through a bus command and the SOC controlling the bus simply routes the data.Normally there will be reach back to the satellite vendor and there may be limited connections to external databases for space situational awareness and data archive services, however connections to external information systems are strictly limited.  | **NIST SP 800-53 Rev. 5** AC-20, PM-5, SA9 |
| ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | Identify and prioritize ground system components, processors, and functions based on their classification, criticality, and value in the context of meeting maintain positive control of the space segment. Provide adequate staffing with the appropriate training such that support is available in a timely manner (consistent with thresholds defined in the organization’s business plan).Stakeholders are advised to use other functions within the CSF to inform the identification and prioritization procedures. For example, while testing business continuity procedures, use the findings to identify which resources of the mission were impacted and to what degree, and reprioritize accordingly.  | **NIST SP 800-37** 3 **NIST SP 800-53 Rev. 5** AC-20, RA-9 |
| ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Third party stakeholder roles does not apply to the SOC. Third party stakeholders and collaborative partners (such as organizations that are hosting a payload) are cryptographically isolated from each other.  | **NIST SP 800-53 Rev. 5** CP-2, PS-7, PM-2, PM-29 |

##### 4.1.2 Business Environment Category

The organization’s mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

There are five Subcategories within Business Environment, four of which apply to the SOC.

| Identify: Business Environment Category |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.BE-1: The organization’s role in the supply chain is identified and communicated | Does not apply to the SOC itself.  | **NIST SP 800-53 Rev. 5** SR-1, SR-3 |
| ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated | Typically, does not apply to the SOC. A payload may provide services that support the critical infrastructure and by extension, the SOC becomes a part of the critical infrastructure.  | **NIST SP 800-53 Rev. 5** PM-8 |
| ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | Does not directly apply to the SOC. Consider communicating the priorities, threshold, and objective performance parameters so that potential customers of the satellite services will understand the scope and suitability for their mission.  | **NIST SP 800-53 Rev. 5** PM-11 |
| ID.BE-4: Dependencies and critical functions for delivery of critical services are established | Identify any critical capabilities form other sectors such as power, transportation, communications etc. that may impact the mission. The organization’s infrastructure, such as network communication architectures, protocols, hardware components, can impact recovery time.Most SOCs have uninterrupted power supplies and diverse communication paths.  | **NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, RA-9 |
| ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | Resiliency requirements for the SOC are strongly dependent on the space and user segments. The ability for the space segment to function autonomously and criticality of the services provided by the payload will define upper and lower bounds on resiliency requirements (such as recovery time, periods of outage etc.)  | **IEC 61850-90-4** 14.2.4 12.2 **NIST SP 800-53 Rev. 5** CP-2, CP-11, RA-9, SA-8RTCA 235 14.2, 14.3, 14.4 |

##### 4.1.3 Governance Category

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.

There are four Subcategories within Governance, all of which apply to the SOC.

| Identify: Governance Category |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.GV-1: Organizational cybersecurity policy is established and communicated | Enables the organization to identify key functions, assign areas of responsibility to ensure a comprehensive cybersecurity approach. | **NIST SP 800-53 Rev. 5** All -1 controls  |
| ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners | Clearly defined internal roles and responsibilities will facilitate a response in a time of duress. Coordination with external partners normally does not apply to the SOC.  | **NIST SP 800-53 Rev. 5** PS-7, PS-9, PM-1, PM-2, PM-29 |
| ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | Maintaining positive control of the space vehicle is critical for collision avoidance, especially for space vehicles that have onboard propellant. The SOC interfaces with the bus or payloads, thus civil liberties and privacy does not apply to the SOC.  | **NIST SP 800-53 Rev. 5** All -1 controls  |
| ID.GV-4: Governance and risk management processes address cybersecurity risks | Develop a comprehensive strategy to manage risk to the SOC. Include cybersecurity considerations in the risk management strategy. For organizations that host payloads, the risk management processes for command and control of the bus may be influenced by changes in the payload mission. Review and update the risk management strategy, as necessary.  | **NIST SP 800-53 Rev. 5**, PM-3, PM-7, PM9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2 **NIST SP 800-160 Rev. 1** 3.3.8**VIM** |

##### 4.1.4 Risk Assessment Category

The organization understands the cybersecurity risk to operations (including mission, functions, image, or reputation), assets, and individuals. In the context of this Profile, the risk to organizational operations in the event of a failure to control or determine the state of health of a satellite or payload is the primary concern.

There are five Subcategories within Risk Assessment, all of which apply to the SOC.

| Identify: Risk Assessment Category |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.RA-1: Asset vulnerabilities are identified and documented. | Identify, document, and report vulnerabilities that exist on the C2 system and the system that transmits commands to and receives acknowledgements from the satellites. Vulnerability scanning is normally done on a representative system, but if safe and feasible may be done on the operational system. Testing and characterization to assess system vulnerabilities are recommended on a periodic basis and when there are modifications to the system. | **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI4, SI-5 |
| ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources. | Commercial entities use resources such as reports generated by vendors, public interest groups or not for profit industry associations. In some cases, threat intelligence may be received from national sources through appropriate channels.  | **ICS-CERT** **NCCIC** **NIST SP 800-53 Rev. 5** PM-15, PM-16 |
| ID.RA-3: Threats, both internal and external, are identified and documented. | Threat identification and documentation is not limited to malicious or threats to information systems. Need to consider natural disasters, accidents etc.  | DIA NASIC NIST SP 800-37 2 NIST SP 800-53 Rev. 5 PM-12, PM16, RA-3, SI-5 NIST SP 800-160 Rev. 1 2.3 RTCA 235 4-12 |
| ID.RA-4: Potential business impacts and likelihoods are identified. | Stakeholders need to be made aware that this type of analysis is probabilistic and typically a range (not a discrete value). The impact analysis needs to be updated as the organization’s business evolves. Likelihood is impacted by externalities such as a time of peace vs. a time of heightened tensions. For malicious threat agents, likelihood is a function of capability and intent. Assessments should be updated as a threat agent’s capabilities increase and events that may affect the intent.  | **NIST SP 800-53 Rev. 5** CP-2, PM9, PM-11, PM-9, RA-2, RA-3, RA-9 RTCA 235 2.1,13 |
| ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. | The risk determination requires a coordinated effort between the threat analysts (for capability and intent of threat agents), system designers (for vulnerability assessment) and mission owner (for impact). The risk should be reassessed on a periodic basis, when there is a substantive change to the system’s vulnerabilities (such as an equipment upgrade), a change in the likelihood of threat realization (such as a time of international tension), a change in the impact should a threat be realized (such as an organization’s increased use or dependency on the satellites’ payload services), and as a result of lessons learned from recovery actions.  | **IETF 8915** 3-9 **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM16, PM-28, RA-2 **NIST SP 800-160 Rev. 1** 2.3, 2.4 **RTCA 235** 2.1-2.4, 3, 14 |
| ID.RA-6: Risk responses are identified and prioritized. | Risk responses may include activities such as increase protection measures, address vulnerabilities through technical or operational means or accept the risk.  | **NIST SP 800-53 Rev. 5**, CA-5, PM-4, PM-9, PM-28, RA-7 |

**4.1.5 Risk Management Strategy**

The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

| Identify: Risk Management Strategy |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders. | Risk management procedures will impact how the SOC conducts its risk assessment process, but not directly applicable to the SOC because establishing these processes must consider the space and user segment as well.  | **NIST SP 800-53 Rev. 5**, PM-9, PM-28 |
| ID.RM-2: Organizational risk tolerance is determined and clearly expressed. | The SOC itself is unlikely to define the organization’s risk tolerance, but the residual risk that is accepted by the SOC will be imposed on the entire organization to some degree. The organizational risk tolerance needs to be clearly expressed to the SOC to avoid an excessive risk to the space and user segments being introduced by the SOC.  | **NIST SP 800-53 Rev. 5**, PM-9 |
| ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | Not directly applicable to the SOC.  | **NIST SP 800-53 Rev. 5**, PM-8, PM-9, PM-11, RA-9 |

**4.1.5 Supply Chain Risk Management Category**

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 established and implemented the processes to identify, assess, and manage supply chain risks.

There are five Subcategories within Supply Chain Risk Management, four of which partially apply to the SOC.

| Identify: Supply Chain Risk Management Category |
| --- |
| Subcategory | Applicability to SOC | References |
| ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. | The SOC will have very constrained external connections and critical components that directly communicate with the space segment will most likely be air gapped. The processes and procedures will need to accommodate unique delivery of updates and patching.  | **NIST SP 800-53 Rev. 5**, PM-30, SA-9, SR-1, SR-2, SR-3, SR-5 |
| ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. | It is unlikely the bus SOC will have third party partner partners. Any use of third parties will be limited and information will be cryptographically isolated (from the partner). Remain apprised of current and future regulations related to the acquisition of services (such as platforms to accommodate a hosted payload), and devices that may form and transport C2 messages or receive payload acknowledgements or telemetry.  | **NDAA** 889**NIST SP 800-161** 2.2, 3**NIST SP 800-53 Rev. 5** PM-9, RA-3, SR-2, SR-3, SR-5, SR-6 |
| ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan. | Supply chain decisions and contracts for systems, components, and services, considerations may include. 1. functional requirements.
2. any relevant and applicable federal law, regulation, or statutory policy.
3. the threat environment.
4. mission-level goals, criticality, and functions;
5. security policies.
6. organizational policies; and
7. the business objectives.
 | **NIST SP 800-53 Rev. 5**, SA-4, SA-9, SR-2, SR-3, SR-5 |
| ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | Assessments and evaluations should be done in the context of supply chain vulnerabilities such as 1. counterfeit systems and components;
2. the development and operational environment; and
3. the logistics or delivery environment.

Consider access paths within the supply chain that would allow adversaries to gain information and introduce hardware, software, or firmware that could cause disruption of the satellite as well as any dependencies that may be easier to exploit. | **NIST SP 800-53 Rev. 5**, AU-6, CA-2, CA-7, PS-7, SA-9, SA-11 |
| ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers | Not applicable to the SOC | **NIST SP 800-53 Rev. 5**, CP-2, CP-4, IR-3, IR-4, IR-8, IR-9 |