**Identify**

* In here, basically it looks at the current systems & data that are being used and evaluate those to identify the potential risks. This includes the identification of the assets & prioritization of them.
* This particular core function consists with multiple sub-categories as following.

1. Asset Management
2. Business Environment
3. Governance
4. Risk Assessment
5. Risk Management Strategy

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Asset Management** | **Inventory physical devices and systems.**  **Ex : -** *computers, mobile devices, networked medical devices, virtual machines* |  |  |  |  |
| **Inventory software platforms and applications.**  **Ex :-** *Microsoft Windows, Mac OS, Linux, Amiga OX* |  |  |  |  |
| **Document the organization’s communication and data flows.** |  |  |  |  |
| **Catalogue externally owned or operated communication systems.**  **Ex :-** *computing devices, wireless networks, and cloud services* |  |  |  |  |
| **Prioritize resources based on their impact to cybersecurity.**  **Ex :-** *hardware devices, data, and software* |  |  |  |  |
| **Outline cybersecurity roles and responsibilities for all employees and 3rd parties.**  **Ex :-** *suppliers, customers, and contractors* |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Business Environment** | **Its function in the supply chain.** |  |  |  |  |
| **Its position in critical infrastructure and the industry.** |  |  |  |  |
| **Information on its mission, objectives and activities.** |  |  |  |  |
| **Dependencies and critical functions for the delivery of critical services.** |  |  |  |  |
| **Recovery requirements and protocols to support critical services.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Governance** | **Information security.** |  |  |  |  |
| **Coordination & alignment of internal and external roles and responsibilities.** |  |  |  |  |
| **Legal and regulatory requirements.** |  |  |  |  |
| **Governance and risk management processes.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Risk Assessment** | **Identify and document asset vulnerabilities.** |  |  |  |  |
| **Receive and share threat and vulnerability information with external organizations.** |  |  |  |  |
| **Document internal and external threats.** |  |  |  |  |
| **Identify potential business impacts.**  **Ex :-** *Likelihood of the threat* |  |  |  |  |
| **Evaluate risks of threats, vulnerabilities, and potential business impact.** |  |  |  |  |
| **Prioritize and respond to identified cybersecurity risks.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Risk Management Strategy** | **Risk management processes approved by organizational stakeholders.** |  |  |  |  |
| **Organizational risk tolerance.** |  |  |  |  |
| **Risk informed processes to determine the acceptable level of risk for the organization’s cybersecurity threats.** |  |  |  |  |