**HW 3 Help your client select NIST CSF controls.**

1. **Identify: (ID)**

Identify helps organization to identify what needs to be protected such as systems, assets, data and capabilities. Identify helps understanding the business context, resources and risk. The activities in the Identify function is sfoundation of the framework for the effective use.

1. Asset Management: (ID.AM)

In asset management the organization identify and manage their importance organizational objectives and the organizations risk strategy. The assets can be data, personal, devices, system and facilities.

1. **ID.AM-2:** Software platforms and applications within the organization are inventoried.

**CIS CSC 2:** Which manages all software on the network so that only authorized software’s can install and execute, **COBIT 5 BAI09.01, BAI09.02, BAI09.05:** It involves management practices like identify and record current assets, managing critical assets, managing licenses, **ISA 62443-2-1-2009:** It applied to the software for industrial automation and control systems describing requirements for each elements.

1. **ID.AM-5:** In this resource are prioritized based on their classification, criticality and business value. Resources can be hardware, data, time, personnel and software. **COBIT 5 APOO3.03, AP003.04, AP012.01, BAI04.02, BAI09.02:** This involves managing enterprise architecture like select opportunities and solutions which define architecture. **ISO**

**ISO/IEC 27001:2013, NIST SP 800-53**

1. **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders. **COBIT 5 AP001.02, DS06.03, ISO/IEC 27001:2013, NIST SP 800-53**
2. **Governance (ID. GV)**

The policies, procedure and process to manage organizations legal, risk, environment and operational requirement which understood and inform the management of cybersecurity risk.

1. **ID.GV-1** Organizational information security policy established. **COBIT 5** APO01.03, EDM01.01, EDM01.02. **ISO/IEC 27001:2013** A.5.1.1. Create, implement, maintain, monitor and enforce a formal and documented Information Security Policy**. NIST SP 800-53 Rev. 4 -1**. NIST SP 800-53 is also known as the Security and Privacy Controls for Information Systems and Organizations**.**
2. **ID.GV-3** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

**COBIT 5** MEA03.01, MEA03.04**. ISO/IEC** 27001:2013 A.18.1. Create, implement, maintain and monitor a comprehensive crossmap which includes legal and regulatory requirements. **NIST SP 800-53 Rev. 4 -1.** NIST SP 800-53 is also known as the Security and Privacy Controls for Information Systems and Organizations

1. **ID.GV-4** Governance and risk management processes address cybersecurity risks. **COBIT 5** DSS04.02. Create, implement, maintain and monitor a comprehensive crossmap which includes legal and regulatory requirements. **NIST SP 800-53 Rev. 4** PM-9, PM-11 Create, implement, maintain, monitor and enforce a formal and documented risk management program, which includes the requirement for risk assessment.

|  |
| --- |
|  |
|  |

|  |
| --- |
|  |
|  |

1. **Risk Assessment (ID.RA)**

The risk that can an organization can have regarding operations, organization assets and individuals.

1. **ID.RA-1** Asset vulnerabilities are identified and documented. ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5. Conduct a formal risk assessment at least annually and after every major change.
2. **ID.RA-3** Threats, both internal and external, are identified and documented. **COBIT** 5 **APO12**.01, APO12.02, APO12.03, APO12.04 Manage risk, risk profiles and key stakeholders. **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16. Complete this work as part of the risk assessment effort.
3. **ID.RA-6** Risk responses are identified and prioritized. **COBIT 5** APO12.05, APO13.02 **NIST SP 800-53 Rev. 4** PM-4, PM-9. Complete this work as part of the risk assessment effort.
4. **Protect: (PR)**

Protect helps to create and implement appropriate safeguards to ensure delivery of critical services. Protect works as a safeguard to limit the impact of a cybersecurity event.

1. **Awareness and training: (PR.AT)**

The training that provides cybersecurity awareness education and information related duties and responsibilities consistent with related policies, procedure and agreements.

1. **PR.AT-1** All users are informed and trained. **ISO/IEC** 27001:2013 A.7.2.2. Create, implement, maintain, monitor and enforce a formal and documented Security Awareness Program for all affected staff and third parties. **NIST SP 800-53 Rev. 4** AT-2, PM-13 Create, implement, maintain and monitor formal and documented targeted training for all affected staff and third parties

1. **PR.AT-2** Privileged users understand roles & responsibilities.

**ISO/IEC** 27001:2013 A.6.1.1, A.7.2.2 Create, implement, maintain, monitor and enforce a formal and documented Security Awareness Program for all affected staff and third parties.

1. **PR.AT-3** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities. **COBIT 5** APO07.03, APO10.04, APO10.05 Create, implement, maintain, monitor and enforce a formal and documented Security Awareness Program for all affected staff and third parties.
2. **Data Security: (PR.DS)**

Data is managed, removed and protected with the organization risk strategy to protect the confidentiality, integrity and availability of information.

1. **PR.DS-1 Data-at-rest is protected. COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 Ensure that affected data is properly encrypted. **ISO/IEC** 27001:2013 A.8.2.3 Ensure that only authorized parties and systems access data.
2. **PR.DS-2** Data-in-transit is protected. **ISO/IEC** 27001:2013 A.8.2.3, A.13.1.1,A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 Ensure that data is communicated electronically in a manner commensurate with its sensitivity.
3. **PR.DS-3** Assets are formally managed throughout removal, transfers, and disposition. **ISO/IEC** 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 Ensure that hardware, software and data are formally tracked.
4. **Information protection processes and procedures: (PR.IP)**

Security policies, processes and procedure are maintained and used to manage protection of information systems and assets.

1. **PR.IP-2** A System Development Life Cycle to manage systems is implemented. **COBIT 5** APO13.01 Create, implement, maintain, monitor and enforce a secure Software Development Lifecycle.

|  |
| --- |
|  |
|  |
|  |
|  |

1. **PR.IP-7** Protection processes are continuously improved.

**NIST SP 800-53** Rev. 4 CA-2, CA-7, CP-2, IR­8, PL-2, PM-6

Evaluate Security Program and implement updates, as required, post-review

|  |
| --- |
|  |
|  |
|  |

1. **PR.IP-9** Response plans and recovery plans are in place and managed. **COBIT 5** DSS04.03 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 Create, implement, maintain, monitor and enforce a formal and documented Business Continuity Management program, to include a Business Impact Analysis and a Business Continuity Plan, along with corresponding processes and procedures
2. **Detect: (DE)**

Detect helps to develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

1. **Anomalies and Events (DE.AE)**

Anomalous activity and events are detected and then potential impact is understood.

1. **DE.AE-1** A baseline of network operations and expected data flows for users and systems is established and managed. **COBIT 5** DSS03.01 Create, implement and maintain a formal and documented network map that includes data flows and detailed information regarding systems, network devices and protocols.
2. **DE.AE-2**: Detected events are analyzed to understand attack targets and methods. **NIST SP** 800-5a3 Rev. 4 AU-6, CA-7, IR-4, SI4 Create, implement, maintain, monitor and enforce a formal Incident Response plan and corresponding procedures.
3. **DE.AE-4** Impact of events is determined. **COBIT 5** APO12.06 Ensure that the logging solution is properly tuned to reflected the impact of events being logged
4. **Security continuous monitoring (DE.CM)**

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

1. **DE.CM-1** The network is monitored to detect potential cybersecurity events. **COBIT 5** DSS05.07 Maintain continuous monitoring of the network, along with targeting vulnerability assessments, including those conducted against sensitive and/or critical areas.
2. **DE.CM-7** Monitoring for unauthorized personnel, connections, devices, and software is performed. **NIST SP** 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 Ensure that continuous logging and scanning are performed in the environment, with alerts being sent to appropriate staff upon discover of anomalous behavior.

1. **DE.CM-8** Vulnerability scans are performed. NIST SP 800-53 Rev. 4 RA-5 Ensure that continuous and targeted vulnerability scanning is performed in the environment, with alerts being sent to appropriate staff upon discover of anomalous behavior.
2. **Detection Processes (DE.AP)**

Detection process and procedures are maintained and tested to remove anomalous events.

1. **DE.DP-2** Detection activities comply with all applicable requirements. **NIST SP** 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 Ensure that logging and monitoring processes conform with the Logging and Monitoring policy; keep processes up-to-date as informed by information on anomalous events experienced by the company
2. **DE.DP-4** Event detection information is communicated to appropriate parties. **ISO/IEC** 27001:2013 A.16.1.2 Ensure that information on event detection is properly communicated during response to incidents; test this communication during the Incident Response testing.
3. **DE.DP-5** Detection processes are continuously improved. **COBIT 5** APO11.06, DSS04.05 Ensure that processes are updated post-review and post-incident, as necessary

1. **Respond: (RS)**

Respond helps to develop and implement appropriate activities or plan to take action in the event of a cybersecurity incident. Respond function supports ability to contain the impact of a potential cybersecurity incident.

1. **Mitigation**

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

1. **RS.MI-1** Incidents are contained. **ISO/IEC** 27001:2013 A.16.1.5 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures.
2. **RS.MI-2** Incidents are mitigated**. ISO/IEC** 27001:2013 A.16.1.5 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures.
3. **RS.MI-3** Newly identified vulnerabilities are mitigated or documented as accepted risks. **ISO/IEC** 27001:2013 A.12.6.1 Ensure that information from incidents is fed into the Vulnerability Management and Risk Management Programs to ensure proper treatment.

1. **Communications**

Response activities are coordinated with internal and external stakeholders to include external support from law enforcement agencies.

1. **RS.CO-1** Personnel know their roles and order of operations when a response is needed. **ISO/IEC** 27001:2013 A.6.1.1, A.16.1.1 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures.
2. **RS.CO-4** Coordination with stakeholders occurs consistent with response plans. **ISO/IEC** 27001:2013 A.16.1.2 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures
3. **RS.CO-**5 Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. **NIST SP** 800-53 Rev. 4 PM-15, SI-5 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures
4. **Analysis**

Analysis is conducted to ensure adequate response and support recovery activities.

1. **RS.AN-1** Notifications from detection systems are investigated. **ISO/IEC** 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures
2. **RS.AN-3** Forensics are performed. Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures.
3. **RS.AN-4** Incidents are categorized consistent with response plans. **NIST SP** 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 Create, implement, maintain, monitor and enforce a formal and documented Incident Response Plan and corresponding processes and procedures.
4. **Recover: (RC)**

Recover means that you have a line of communication and activities in place to restore any system capabilities or services that has been affected in a cybersecurity event.

1. **Recovery Planning (RC.RP)**

Recovery processes and processes and procedures are executed and maintained to ensure restoration of systems or assets if it’s affected by the cybersecurity events.

1. **RC.RP-**1 Recovery plan is executed during or after an event. **ISO/IEC** 27001:2013 A.16.1.5 Create, implement, maintain, monitor and enforce a formal Business Continuity/Disaster Recovery (BCDR) Plan(s) and corresponding processes and procedures for recovery.
2. **Improvements (RC.IM)**

Recovery planning and processes are improved by incorporating encountered cyber threats and future activities.

1. **RC.IM-1** Recovery plans incorporate lessons learned. **COBIT 5** BAI05.07 Update BCDR Plan after each response to ensure response is optimized
2. **RC.IM-2** Recovery strategies are updated. **NIST SP** 800-53 Rev. 4 CP-2, IR-4, IR-8 Create, implement, maintain, monitor and enforce a formal Business Continuity/Disaster Recovery (BCDR) Plan(s) and corresponding processes and procedures for recovery
3. **Communications (RC.CO)**

Restoration activities are coordinated with internal and external parties.

1. **RC.CO-1**: Public relations are managed.  **COBIT 5** EDM03.02 Create, implement, maintain, monitor and enforce a formal Business Continuity/Disaster Recovery (BCDR) Plan(s) and corresponding processes and procedures for recovery
2. **RC.CO-2**: Reputation after an event is repaired. **COBIT 5** MEA03.02 Create, implement, maintain, monitor and enforce a formal Business Continuity/Disaster Recovery (BCDR) Plan(s) and corresponding processes and procedures for recovery.
3. **RC.CO-3**: Recovery activities are communicated to internal stakeholders and executive and management teams. **NIST SP** 800-53 Rev. 4 CP-2, IR-4 Create, implement, maintain, monitor and enforce a formal Business Continuity/Disaster Recovery (BCDR) Plan(s) and corresponding processes and procedures for recovery.