Cybersecurity Framework Security Policy Mapping Table

The following table illustrates how specific requirements of the US Cybersecurity Framework [1] are addressed by the ISO 27002 standard and covered by sample policy documents within Information Security Policies Made Easy (ISO 27002). In most cases, a single document covers more than a single subcategory requirement.

Function	Category	Subcategory	CPL Sample Policy
IDENTIFY (ID)	**Asset Management (AM):** The personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.		**Asset Management Policy** ISO 27002 - 8.1. Responsibility for assets
	AM	**ID.AM-1**: Physical devices and systems within the organization are inventoried	8.1.1 Inventory of assets
	AM	**ID.AM-2:** Software platforms and applications within the organization are inventoried	8.1.1 Inventory of assets
	AM	**ID.AM-3:** The organizational communication and data flow is mapped	
	AM	**ID.AM-4:** External information systems are mapped and catalogued	
	AM	**ID.AM-5:** Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software	**Information Classification Policy** 8.2 Information classification
	AM	**ID.AM-6:** Workforce roles and responsibilities for business functions, including cybersecurity, are established	**Information Security Organization Policy** 6.1.1 Information security roles and

			responsibilities
ID	**Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized, and inform cybersecurity roles, responsibilities, and risk decisions.		**Information Security Planning Policy** ISO 27002 - 6.1 Internal organization
	BE	**ID.BE-1:** The organization’s role in the supply chain and is identified and communicated	
	BE	**ID.BE-2:** The organization’s place in critical infrastructure and their industry ecosystem is identified and communicated	
	BE	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established	5.1 Management direction for information security
	BE	**ID.BE-4**: Dependencies and critical functions for delivery of critical services are established	17.1.1 Planning information security continuity
	BE	**ID.BE-5**: Resilience requirements to support delivery of critical services are established	17.2 Redundancies
ID	**Governance (GV):** 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.		**Information Security Program Policy** **ISO -** 5.1. Management direction for information security
		ID.GV-1: Organizational information security policy is established	5.1.1 Policies for information security
		ID.GV-2: Information security roles & responsibility are coordinated and aligned	**Information Security Organization Policy** 6.1.1 Information security roles and responsibilities
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	18.1 Compliance with legal and contractual requirements
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**IT Risk Management Policy**

			4 Risk Assessment
ID	**Risk Assessment (RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.		**IT Risk Management Policy** ISO 27002: 4.0 Risk Management
	RA	**ID.RA-1:** Asset vulnerabilities are identified and documented	
	RA	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources.	
	RA	**ID.RA-3:** Threats to organizational assets are identified and documented	
	RA	**ID.RA-4:** Potential impacts are analyzed	
	RA	**ID.RA-5**: Risk responses are identified.	
ID	**Risk Management Strategy (RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. .		**IT Risk Management Policy** ISO 27002: 4.0 Risk Management
	RM	**ID.RM-1:** Risk management processes are managed and agreed to	
	RM	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed	
	RM	**ID.RM-3**: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	
PROTECT (PR)	**Access Control (AC):** Access to information resources and associated facilities are limited to authorized users, processes or devices (including other information systems), and to authorized activities and transactions.		**Access Control Policy** ISO 27002 - 9. Access control
	AC	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**Account Management Policy** 9.2 User access management
	AC	**PR.AC-2:** Physical access to resources is managed and secured	**Physical Access Security Policy**

			11.1.2 Physical entry controls
	AC	**PR.AC-3:** Remote access is managed	**Remote Access Security Policy** 9.1.2 Access to networks and network services
	AC	**PR.AC-4:** Access permissions are managed	9.2.2 User access provisioning
	AC	**PR.AC-5:** Network integrity is protected	**Network Security Policy** 9.1.2 Access to networks and network services
	Awareness and Training (AT): The organization's personnel and partners are adequately trained to perform their information security- related duties and responsibilities consistent with related policies, procedures, and agreements.		**Security Awareness and Training Policy** ISO 27002: 7.2.2 - Information security awareness, education and training
PR		**PR.AT-1:** General users are informed and trained	
		PR.AT-2: Privileged users understand roles & responsibilities	
		PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities	**Third Party Security Management** 15.1.1 Information security policy for supplier relationships
		PR.AT-4: Senior executives understand roles & responsibilities	
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	
PR	**Data Security (DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		**Information Protection Policy**
		PR.DS-1: Data-at-rest is protected	**Information Protection Policy** 8.2.3 Handling of assets
		PR.DS-2: Data-in-motion is secured	**Information Exchange Policy**

PR		8.3.3 Physical media transfer
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**Asset Management Policy** 8.2.3 Handling of assets
	PR.DS-4: Adequate capacity to ensure availability is maintained.	**Operational Security Policy** 12.1.3 Capacity management
	PR.DS-5: There is protection against data leaks	8.1.3 Acceptable use of assets
	PR.DS-6: Intellectual property is protected	**Acceptable Use of Assets** 18.1.2 Intellectual property Rights
	PR.DS-7: Unnecessary assets are eliminated	
	PR.DS-8: Separate testing environments are used in system development	**Application Development Security Policy** 14.3.1 Protection of test data
	PR.DS-9: Privacy of individuals and personally identifiable information (PII) is protected	**Data Privacy Policy** 18.1.4 Privacy and protection of personally identifiable information
	Information Protection Processes and Procedures (IP): Security policy (that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets	**Information Security Program Policy** ISO 27002 – 14. System acquisition, development and maintenance & ISO 27002: 12 Operations security
	PR.IP-1: A baseline configuration of information technology/operational technology systems is created	**System Configuration Management Policy** 14.2 Security in development and support processes
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	**System Configuration Management Policy** 14.2.1 Secure development policy
	PR.IP-3: Configuration change control processes are in	**Change Control Policy**

PR		place	12.1.2 Change management
		PR.IP-4: Backups of information are managed	**Information Backup Policy** 12.3.1 Information backup
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	**Physical Security Policy** 11.2.1 Equipment siting and protection
		PR.IP-6: Information is destroyed according to policy and requirements	**Information Disposal Policy** 8.3.2 Disposal of media
		PR.IP-7: Protection processes are continuously improved	18.2.3 Technical compliance review
		PR.IP-8: Information sharing occurs with appropriate parties	**Information Exchange Security Policy** 13.2.2 Agreements on information transfer
		PR.IP-9: Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed	**IT Continuity Security Policy** 17.1 Information security continuity
		PR.IP-10: Response plans are exercised	17.1.3 Verify, review and evaluate information security continuity
		PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	**Personnel Security Management Policy** 7.1.1 Screening
	Maintenance (MA): Maintenance and repairs of operational and information system components is performed consistent with policies and procedures.		**Physical Security Policy** ISO 27002 - 11.2.4 Equipment maintenance
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	11.2.5 Removal of assets
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability	11.2.6 Security of equipment and assets off premises

	requirements for important operational and information systems.	
PR	**Protective Technology (PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**Log Management Security Policy** 12.4 Logging and monitoring
	PR.PT-1: Audit and log records are stored in accordance with audit policy	**Log Management Security Policy** 12.4 Logging and monitoring
	PR.PT-2: Removable media are protected according to a specified policy	**Removable Media Policy** 8.3.1 Management of removable media
	PR.PT-3: Access to systems and assets is appropriately controlled	**Access Control Policy** 9.1.2 Access to networks and network services
	PR.PT-4: Communications networks are secured	**Network Security Policy** 13.1 Network security management
	PR.PT-5: Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS)	
DETECT (DE)	**Anomalies and Events (AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. .	**System Monitoring Security Policy** ISO 27002 - 12.4 Logging and monitoring
	DE.AE-1: A baseline of normal operations and procedures is identified and managed	12.1.1 Documented operating procedures
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	16.1.2 Reporting information security events
	DE.AE-3: Cybersecurity data are correlated from diverse information sources	16.1.2 Reporting information security events
	DE.AE-4: Impact of potential cybersecurity events is determined.	16.1.4 Assessment of and decision on information security events

	DE.AE-05: Incident alert thresholds are created	16.1.2 Reporting information security events
DE	**Security Continuous Monitoring (CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**System Monitoring Security Policy** ISO 27002 - 12.4.1 Event logging
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**Physical Security Policy** 11.1.1 Physical security perimeter
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**System Monitoring Security Policy** 11.1.3 Securing offices, rooms and facilities
	DE.CM-4: Malicious code is detected	**Malicious Software Management Policy** 12.2.1 Controls against mal-Ware
	DE.CM-5: Unauthorized mobile code is detected	**Malicious Software Management Policy** 12.2.1 Controls against mal-Ware
	DE.CM-6: External service providers are monitored	**Third Party Security Policy** 15.2 Supplier service delivery management
	DE.CM-7: Unauthorized resources are monitored	
	DE.CM-8: Vulnerability assessments are performed	**System Monitoring Security Policy** 18.2.3 Technical compliance review
DE	**Detection Processes (DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**Incident Management Security Policy** ISO 27002: 16. Information security incident management
	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	16.1.1 Responsibilities and Procedures
	DE.DP-2: Detection activities comply with all applicable requirements, including those related to privacy and civil liberties	18.1.1 Identification of applicable legislation and contractual requirements

	DE.DP-3: Detection processes are exercised to ensure readiness	16.1.5 Response to information security incidents
	DE.DP-4: Event detection information is communicated to appropriate parties	6.1.3 Contact with authorities
	DE.DP-5: Detection processes are continuously improved	16.1.6 Learning from information security incidents
RESPOND (RS)	**Response Planning (RP):** Response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events.	**Security Incident Management Policy** ISO - 16. Information security incident management
	RS.PL-1: Response plan is implemented during or after an event.	
RS	**Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies.	**Security Incident Management Policy** 16.1.1 Responsibilities and Procedures ISO - 6.1.3 Contact with authorities
	RS.CO-1: Personnel know their roles and order of operations when a response is needed	16.1.1 Responsibilities and Procedures
	RS.CO-2: Events are reported consistent with established criteria	16.1.2 Reporting information security events
	RS.CO-3: Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties	16.1.5 Response to information security incidents
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties	6.1.4 Contact with special interest groups
	RS.CO-5: Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	6.1.3 Contact with authorities
RS	**Analysis (AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**Security Incident Management Policy** ISO - 16.1.4 Assessment of and decision on

			information security events.
		RS.AN-1: Notifications from the detection system are investigated	
		RS.AN-2: Understand the impact of the incident	
		RS.AN-3: Forensics are performed	
		RS.AN-4: Incidents are classified consistent with response plans	
RS	**Mitigation (MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.		**Security Incident Management Policy** ISO - 16.1.5 Response to information security incidents
	MI	**RS.MI-1:** Incidents are contained	
	MI	**RS.MI-2:** Incidents are eradicated	
RS	**Improvements (IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.		**Security Incident Management Policy** ISO - 16.1.6 Learning from information security incidents
	IM	**RS.IM-1:** Response plans incorporate lessons learned	
	IM	**RS.IM-2:** Response strategies are updated	
RECOVER (RC)	**Recovery Planning (RP):** Recovery processes and procedures are maintained and tested to ensure timely restoration of systems or assets affected by cybersecurity events.		**IT Continuity Security Policy** ISO 27002: 17.1 Information security continuity
	RP	**RC.RP-1:** Recovery plan is executed	17.1.2 Implementing information security continuity
	Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.		**IT Continuity Security Policy** ISO 17.1.3 Verify, review and evaluate information security continuity
	IM	**RC.IM-1:** Plans are updated with lessons learned	

	IM	**RC.IM-2:** Recovery strategy is updated	
	Communications (CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other		**IT Continuity Security Policy** ISO - 16.1.5 Response to information security incidents ISO - 6.1.3 Contact with authorities
	CO	**RC.CO-1:** Public Relations are managed	6.1.4 Contact with special interest groups
	CO	**RC.CO-2:** Reputation after an event is repaired	