Use Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at Idaho State University, I agree that the Library shall make it freely available for inspection. I further state that permission to download and/or print my thesis for scholarly purposes may be granted by the Dean of the Graduate School, Dean of my academic division, or by the University Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature _____

Date _____

A FRAMEWORK FOR CROSSREFERENCING BUSINESS INJECTS USED IN CYBER COMPETITIONS TO INDUSTRY STANDARDS

By

Albert Ray Fox Jr

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Business Administration in the College of Business

Idaho State University

Spring 2014

Committee Approval

To the Graduate Faculty:

The members of the committee appointed to examine the thesis of JANE STUDENT find it satisfactory and recommend that it be accepted.

_____

Dr. Corey Schou,
Major Advisor

_____

Dr. Dennis Krumweide,
Committee Member

_____

Dr. Dorothy Sammons,
Graduate Faculty Representative

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank all the people who are responsible for the successful completion of this project.

I express my sincere gratitude to Dr. Corey Schou and Dr. James Frost for giving me an opportunity to work under their guidance. This project helped me learn something very new, which I have not learned in my coursework.

I would like to thank all the NIATEC team members for providing their valuable insight into the development of effective injects.

I thank my wife Michelle for her continuous support.

CONTENTS

List of Tables

A FRAMEWORK FOR CROSS-REFERENCING BUSINESS INJECTS USED IN CYBER COMPETITIONS TO INDUSTRY STANDARDS

Thesis Abstract-Idaho State University (2014)

Many institutions, both at high school and collegiate levels, include cyber exercises as a part of their curricula. These competitions provide an environment to learn the real-time and lifelike scenarios such as defending security loopholes and adding new software or services as a typical IT company would do. The outcomes and assessment of the exercises do not generally include the mapping of the exercises to specific standards. While competitors are obtaining valuable skill sets in information assurance, the resulting competencies are not as quantifiable as those from more standard types of educational activities such as uniform quizzes and exams. This thesis will create a framework for the development of injects that are directly related to controls across multiple standards. This framework facilitates the use of cyber exercises as a foundational component in the education of the information assurance professional, while providing consistent outcomes that can be measured against standards.

Chapter 1 Introduction

1.1 Cyber Defense Competition (CDC)

During 2001, the United States military academy created an academic exercise which could be termed as the originating point of Cyber Defense Competition (CDC). A cyber defense competition is a competition where teams compete and learn how to defend a system to better understand how things work in real time. There are other types of competitions known as “Capture the Flag” and “Attack/Defend” events. “Capture the flag” is based on flags associated with services. Whoever sets the flag for a service would get the points. The “Attack/Defend” competition requires a team to both defend their network and infiltrate the opposing team’s network. In a Cyber Defense Competition, the blue team (competitor) is assigned a group of server machines which they have to defend, as the red team (attackers) tries to break into those machines. Defenders must be capable of securing their network as well as machines so that attackers cannot hack into their systems. If attackers gain access to the systems of defenders, the line defenders lose points when they fail to maintain the security of their systems. The defenders score points or can balance the points they lost by working on Injects.

Injects are business tasks they have to perform. The white team gives these tasks at frequent time intervals which students have to perform within a certain time constraint. These injects are designed to resembles the normal work load in a typical IT department. (Dodge R.C. Jr. H. B., 2009)

Since there is a need for these competitions to get hands-on experience, there is a similar need to develop injects that have direct relevance to industry standards. Certifications, like the CISSP (Certified Information Systems Security Professional), show a skill level across a range of standards. The outcome of a CDC (Cyber Defense Competition) should show more than a winner; it should convey a level of competency that can be measured against a standard.

To measure the effectiveness of cyber security exercises, a set of metrics is needed. The effectiveness of the exercise expresses how well the objectives have been achieved. Therefore, the chosen metrics should be tightly related to the objectives. On the other side, the objectives should be expressed in measurable terms.

This project aims at providing a framework that can be used for one of these metrics. The framework will cross-reference injects to different industry standards and certifications. The proposed system provides a simplified user interface which is useful in developing new injects and linking them to industry standards; it will also provide the ability to add additional standards as they are developed.

The report is further organized as follows: Chapter 2 provides information about Industry Standards. Chapter 3 describes Cyber Competitions and team assignments. Chapter 4 covers the framework and database design. Chapter 5 provides the user guide and site

map for the web pages. Chapter 6 concludes the report. It also includes the summary of the work.

1.2 Business Inject

Information and computer security is one of the main aspects of today's enterprise level IT infrastructure. Every company should strive to maintain high security and availability to provide uninterrupted services to their customers. Every field in today's hyper connected world is automated using a wide range of computer systems for example, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors that include in part: chemical sector, commercial facilities sector, communications sector, defense industrial base sector, emergency services sector, energy sector, and financial services sector. (DHS) As industry becomes aware and trains for computer security, we also need personnel who are trained in the security domain to keep track of the problems and to secure the network from attackers. These personnel should learn to perform these tasks in hostile conditions created by attackers who try to break the security and perform malicious activities.

A business inject, in reference to Cyber Defense Competitions, is a task that can be expected to occur during a normal business day. An example of an "inject" is: "Create a user account that has limited access for a visiting inspector." The implied tasks in this

inject are: assigning a name, setting duration for the access, and placing the individual in a group policy that allow the correct level of access to complete the work. These can be policy oriented, technically driven, or report based. A Cyber Defense Competition is a closed environment that tests the ability of a "Team" of IT professionals to defend and protect their environment while maintaining the level of availability of services required by predefined rules.

Chapter 2 Industry Standards

The term "standard" is sometimes used interchangeably within the context of information security to mean policies, standards, and procedures. In order for an organization to secure their environment, all three levels of documentation need to be employed. Policies are high-level statements or rules about protecting people or systems. For example, a policy would state that "Two factor authentications are required for entry into the facility." A "standard" is a minimum requirement that must be met to comply with the policy. For example, “Users must use an access card and enter a pin for access.” A "procedure" can describe a step-by-step method to implementing various standards. For instance, "All employees will be issued key cards and select a personal pin on the first day of hire.”

2.1 Certified Information Systems Security Professional (CISSP)

A CISSP is an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business environments. The credential demonstrates a globally recognized level of competence provided by the $(ISC)^2$® CBK®, which covers critical topics in security today, including: cloud computing, mobile security, application development security, risk management, and more.

CISSP was the first credential in the field of information to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement (ICS2 CISSP information).

The CISSP curriculum covers subject matter in a variety of Information Security topics. The CISSP examination is based on what (ISC)² terms the Common Body of Knowledge (or CBK). According to (ISC) ², "the CISSP CBK is a collection of topics relevant to information security professionals around the world. The CISSP CBK establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss debate and resolve matters pertaining to the profession with a common understanding." (ICS2 CISSP information)

Currently, the CISSP certification covers the following ten domains:

1. Access control
2. Telecommunications and network security
3. Information security governance and risk management
4. Software development security
5. Cryptography
6. Security architecture and design
7. Operations security
8. Business continuity and disaster recovery planning
9. Legal, regulations, investigations and compliance
10. Physical (environmental) security

2.2 Federal Information Security Management Act of 2002 (FISMA)

FISMA stands for Federal Information Security Management Act, and is a part of the US E-Government Act (Public Law 107-347) that became legislation in 2002. It requires US

federal agencies to develop, document, and implement an agency-wide program to provide information security for the information (and information systems) that support the operations and assets of the agency. Some of the requirements include:

1. Periodic risk assessments of information and information systems that support the operations and assets of the organization.

2. Risk-based policies and procedures designed to reduce information security risks to an acceptable level.

3. Plans for providing adequate security for networks and information systems.

4. Security awareness training to all personnel, including contractors.

5. Periodic evaluation and testing of the effectiveness of the security policies, procedures and controls. The frequency should not be less than annually. Remedial action to address any deficiencies found to be properly managed.

6. A working and tested security incident handling procedure.

7. A business continuity plan in place to support the operation of the organization. (Region, 2008)

2.3 Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA. FIPS Publication 199, Standards for Security Categorization of Federal

Information and Information Systems, is the first mandatory security standard laid down under the FISMA legislation. FIPS Publication 200, entitled "Minimum Security Requirements for Federal Information and Information Systems" is the second mandatory set of security standards that specify minimum security requirements for US federal information and information systems across seventeen security-related areas. US federal agencies must meet the minimum security requirements defined in this standard by selecting appropriate security controls and assurance requirements laid down in NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) (Region, 2008).

2.4 National Institute of Standards and Technology (NIST)

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST Special Publication 800-53 contains a list of controls to be implemented for added security:

2.5 International Organization for Standardization (ISO)

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards.

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature (ISO).

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Source: (ISO)

2.6 Control Objectives for Information and related Technology (COBIT)

The Control Objectives for Information and related Technology (COBIT) is “a control framework that links IT initiatives to business requirements, organizes IT activities into a

generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered"

COBIT 4.1 consists of 7 sections, which are:

1. Executive overview
2. COBIT framework
3. Plan and Organize
4. Acquire and Implement
5. Deliver and Support
6. Monitor and Evaluate
7. Appendices and glossary

Its core content can be divided according to the 34 IT processes. COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks around IT security in a way that is simple to follow and implement for small and large organizations (Region, 2008).

2.7Sarbanes-Oxley Act

After a number of high-profile business scandals in the US, including Enron and WorldCom, the Sarbanes-Oxley Act of 2002 (SOX) was enacted as legislation in 2002. This act is also known as the "Public Company Accounting Reform and Investor Protection Act". The purpose is to "protect investors by improving the accuracy and

reliability of corporate disclosures made pursuant to the securities laws, and for other purposes." This regulation affects all companies listed on stock exchanges in the US.

In section 404, the SOX require "each annual report … contain an internal control report … [that] contains an assessment of … the effectiveness of the internal control structures and procedures of the issuer for financial reporting." As information technology plays a major role in the financial reporting process, IT controls would need to be assessed to see if they fully satisfy this SOX requirement.

Although information security requirements have not been specified directly in the Act, there would be no way a financial system could continue to provide reliable financial information, whether due to possible unauthorized transactions or manipulation of numbers, without appropriate security measures and controls in place. SOX requirements indirectly compel management to consider information security controls on systems across the organization in order to comply with SOX (Region, 2008).

The controls for SOX are developed in the COSO (Committee of Sponsoring Organizations). The development of this framework is not the only acceptable one to meet the requirements of SOX.

2.8 Committee of Sponsoring Organizations of the Treadway Commission

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework is a framework that initiates an integrated process of internal controls. It helps improve ways of controlling enterprises by evaluating the effectiveness of internal controls. It contains five components:

1. Control Environment, including factors like integrity of people within the organization and management authority and responsibilities;

2. Risk Assessment, aiming to identify and evaluate the risks to the business;

3. Control Activities, including the policies and procedures for the organization;

4. Information and Communication, including identification of critical information to the business and communication channels for delivering control measures from management to staff;

5. Monitoring, including the process used to monitor and assess the quality of all internal control systems over time. (Region, 2008)

2.9 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a US law designed to improve the portability and continuity of health insurance coverage in both the group and individual markets, and to combat waste, fraud, and abuse in health insurance and health care delivery as well as other purposes. The Act defines security standards for healthcare information, and it takes into account a number of factors including the technical capabilities of record systems used to maintain health information, the cost of security measures, the need for training personnel, the value of audit trails in computerized record systems, and the needs and capabilities of small healthcare providers.

A person who maintains or transmits health information is required to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of that information. In addition, the information should be properly protected from threats to the security and integrity of that information, unauthorized uses, or unauthorized disclosure (Region, 2008).

Administrative Safeguards

Security Management Process. As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel. A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Information Access Management. Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

Workforce Training and Management. A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

Facility Access and Control. A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Technical Safeguards

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network (Region, 2008).

Chapter 3 Team Assignments and Cyber Competitions

3.1 Team Assignments

3.1.1 White Team

The White Cell develops the scenarios and injects, established the scoring criteria, referees the exercise, and determines the winner based on the effectiveness of each team's ability to minimize the impact to their network of the Red Forces malicious activities.

The competition begins with identical systems set up for each Blue Team. The systems are designed with multiple flaws to force teams to prioritize the hardening of their systems. Without warning, anomalies are injected into the scenario. These operational irregularities test the student teams and their system ability to react on the fly. They can be as complex as requiring each team to stand up an anonymous Email server based on company specifications to as simple as requiring a new user be added to the system. Whatever the anomaly, all participants are exposed equally and their actions, procedures, and policies to address them are evaluated (Schepens W.J. J. J., 2003).

3.1.2 Red Team

The Red Teams provides the insider and outsider threat during the cyber defense exercise. They are the attackers working to penetrate the Blue Team systems. The Red Team is given a range of IPs as a battlefield surface. Depending on the length and type

of the exercise additional information can be given to the Red Team to help focus the process.

3.1.3 Blue Team

The Blue Teams are the competitors. Most competitions begin with a group of IT professionals taking authorized control of an established system. The level of information available is event specific. For example a one day event might provide a complete network map with all updates installed on all machines. A longer event might only provide a short list of services that must be maintained.

3.1.4 Black Team

The Black Team assembles the hardware and software to build the systems designed by the White Team. This team is responsible for the development and testing of the system to ensure they are working as designed prior to any assault but the Red Team. 3.2 Cyber competitions

3.2.1 Defensive

In a defensive game, student participants do not engage in any attacking activities. Penetration attacks are performed by a team of judges often referred to as the red team. Many proponents of defensive games are uncomfortable with ethical risks associated with teaching cyber attacking techniques in a university curriculum. Proponents of offensive games believe that a good understanding of attacking methods is essential for designing effective defenses and the risks associated with teaching attack techniques can be mitigated through appropriate ethics education (Chu, 2007).

3.2.2 Defense vs. Offensive Game

In an offensive game, student participants engage in activities that attempt to penetrate computer systems. A red team is optional and often not used in offensive games. Participants often engage in defensive activities as well in offensive games. Many proponents of defensive games are uncomfortable with ethical risks associated with teaching cyber attacking techniques in a university curriculum. Proponents of offensive games believe that a good understanding of attacking methods is essential for designing effective defenses and the risks associated with teaching attack techniques can be mitigated through appropriate ethics education (Chu, 2007).

3.2.3 Capture the flag

In a Capture the Flag game, opposing teams attempt to end the game with the most flags set in the network. The defensive part is to protect the flags you have set and thus prevent your opponent from making the switch. The offensive part is not to disrupt service, but to take over the service for your use.

3.3 Define Exercise Objectives

Defining the exercise objectives is the starting point for the design of the cyber security exercise. All of the steps of the exercise design depend on the chosen objectives and are influenced by them. The objectives for a cyber-security exercise can be split in two main categories, according to the type of security training desired – offensive security or defensive security. The defensive security training prepares the participants for the

generic job of security administrator. Their main goal is to be experts in configuring and managing various securities equipment's. The best example for this kind of practical training is the annual "Cyber Defense Exercise" organized by the US Military Academy at WestPoint. In the development of a competition more emphasis should to be placed on linking the business injects to the standard the controlling authority of the competition subscribes to.

Chapter 4 Framework

4.1 Associating Domains to Standards

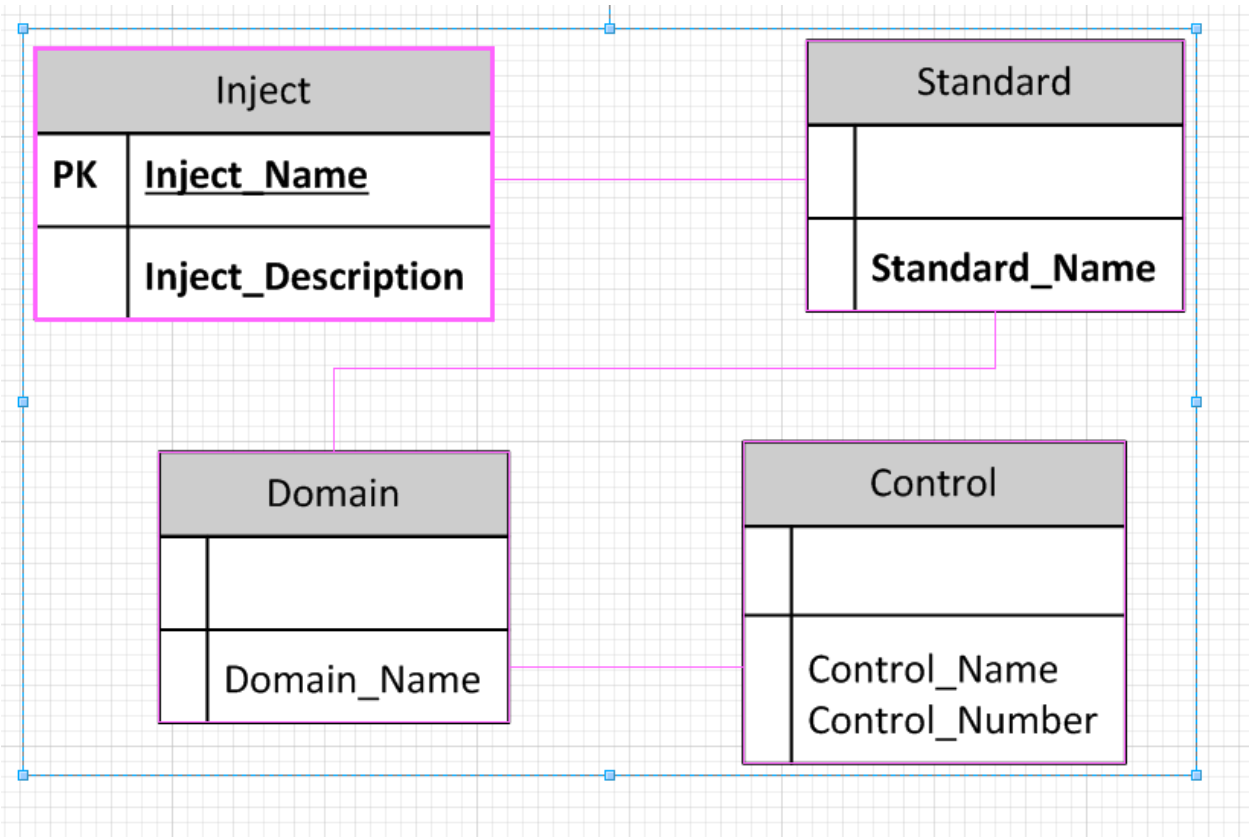
My framework allows for growth by adding more standards. As new standards are developed, an initial analysis need to be accomplished. This analysis must map the "new" standard to the existing domains and controls.

The tables listed in the appendix show the relationships between multiple standards. Table 1 indicates domains that are consistent across the standards. The Second Table was developed by DHS and does not strictly follow the domains of table 1 but is more focused on COBIT ISO and NIST controls. This cross-referencing clearly outlines that multiple standards have identical requirements. The third table provides a cross reference of ISO controls to NIST controls found in SP 800-53.

The input of an Inject, based on a standard, into the software will automatically link it to all the standards in the system. Once this data base is built, you can select the standard you want to train for and the system will output injects that will test the domains and controls.

4.2 Data Base

The database build is included in the appendix below. There are very few tables needed to accomplish my task framework. The four main tables that are needed are Injects, Domains, Controls, and Standards. Additionally, tables are needed to link the base tables. Every base table has a many to many relationship with each other base table.



4.3 Use Cases

4.3.1 Standard

The primary use of the cross referencing data base is to determine what injects to use for a CDC. If a competition is being designed to meet a specific standard, the standard can be queried in the data base and a list of injects will be returned that are mapped to corresponding domains and controls of that standard.

In the example give below FISMA is the standard that is being used for a Cyber Defense Competition. The search for FISMA injects returns a list of eleven injects that will help test participants knowledge of FISMA requirements.

- Standard – FISMA
- Injects-
  - Data Class & Labeling
  - Warning Banners Implementation and Check
  - Password Policy
  - Complete Network Map
  - Encrypted Blueprints
  - Whaling Response and Training
  - Disable USB on Computers
  - Board of Directors - Presentation on BYOD
  - User verification over phone
  - Change Log
  - Call Log

4.3.2 Inject

The creation of an inject is currently done in the boundary of the current competition. With the development of this framework and database, an inject can be

searched for and all related Domains and Controls across multiple standards will be identified.

In the following example if a search was done for the inject “Password Policy”, this is the response that would be returned. In this example only if you were training to the HIPAA standard you can see there is no Control that maps to a Password Policy Inject.

- ⊡ Inject- Password Policy
- ⊡ Domain – Access Control
- ⊡ Control –
  - COBIT 5 APO01.03, EDM01.01, EDM01.02
  - ISA 62443-2-1:2009 4.3.2.6
  - ISO/IEC 27001:2013 A.5.1.1
  - NIST SP 800-53 Rev. 4 -1 AC-1 Access Control Policy and Procedures

4.3.3 Control

Not all standards have the granularity of controls. Some are limited to simply having Domains and rely on best practices to develop the controls to meet the domain requirement.

The following example shows that the search for the Domain “Access Control” provides the following results. It is clear that HIPAA is a standard that has the domain of Access Control and that one of the injects associated with that Domain is Password Policy.

Domain

- Domain - Access Control
- Standards-
  - CISSP
  - NIST
  - ISO
  - HIPAA
- Injects-
  - Password Policy
  - Disable USB on Computers
  - User verification over phone

Chapter 5 Conclusion

Corporations and governments are well beyond the initial stages of recognizing the need to provide digital protection. This acknowledgement is reflected in the development of standards. Most of the standards that have been developed have similar requirements. Often a requirement is simply a rewording of a control from a different standard. Centers of higher education also acknowledge the need to protect digital systems and have developed cyber defense competitions (CDC) to test the skills of their students.

My cross-referencing framework seeks to address the disconnect between tasks that are expected to occur during normal business operations, business injects, used in different CDCs and link them to the information security standards that are applicable. Its concept is derived from research and consideration of multiple types of CDCs and established standards. The core of the model lies in reuse of business injects that have been proven effective. Injects are not normally shared from one competition to another, rather they are treated like proprietary knowledge. The next logical step is to open the database for use and encourage the addition of injects and standards.

References

(NIST), N. I. (1995, October NA). Special Pub 800-12 -- An Introduction to Computer Security: The

NIST Handbook. Washington D.C., District of Columbia, USA.

Aaron Blum, B. W. (2010). Lexical Feature Based Phishing URL Detection Using Online Learning. *AISec '10 Proceedings of the 3rd ACM workshop on Artificial intelligence and security*, 54-60.

Adams W.J., G. E. (2009). *Collective Views os the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives.* Colorado Springs: US Air Force Academy.

Albert, R. (2010). The U in Information Security. *Proceedings of the 2009 ASCUE Summer Conference*, (pp. 23-31).

Armstrong C.J., A. H. (2007). Mapping information Security Curricula to Professional Accreditation Standards. *Proceeding of the 2007 IEEE*, 30-35.

Augustine T.A., D. L. (2010). Cyber Competitions As a Computer Science. Annapolis: United States Naval Academy.

Augustine, T. a. (2006). Cyber Defense Exercise: Meeting Learning Objectives thru Competition. *Proceeding of 10th Colloquium for information Systems Security Education,.*

Bei Y., K. R. (2011). Cyber Defense Competition: A Tale of Two Teams. *Journal for Computing Sciences in Colleges*.

Biggers, M. B. (2008). Student perceptions of computer science: a retention study comparing graduating seciors with cs leavers. *39th SIGCSE Technical Symposium on Computer Science Education*, (pp. 402-406).

Boleng J., S. D. (2008). *Developing Cyber Warriors.* Colorado Springs : US Air Force Academy.

Burnes, B. (2004). Kurt Lewin and the Planned Approach to Change: A Re-appraisal. *Journal of Managment Studies 41:6*, 977-1002.

Carter, L. (2006). Why students with an apparent aptitude for computer science don't choose to major in computer science. *37th SIGCSE*, (pp. 27-31).

Cavanagh C., A. R. (n.d.). *Goals, Models, and Progress towards Establishing a Virtual Information Security Laboratory in Maine.* Fort Kent: Universtiy of Maine.

Chu, B.-T. A.-J. (2007). Collegiate Cyber Game Design Criteria and Participation. *6th IEEE?ACIS International Conference on Computer and Information Science.*

Collegiate Cyber Defense Competition. (2013). Retrieved Oct 2013, from National Collegiate Cyber Defense Competition: www.nationalccdc.org

Conklin, A. (2005). the use of a collegiate cyber defense competition in informarion securtiy education. *Proceedings of the 2nd Annual Conference on information Security Curriculum Develompent*, (pp. 16-18).

Conklin, A. (2006). Cyber Defrense Competitions and Information Security Education: An Active Learning Solution for a Capstone course. *39th Hawaii International Conferance on System Sciences.*

DC206. (n.d.). Retrieved Oct 2013, from Pacific Rim Collegiate Cyber Defense Competition overview: http://www.dc206.org/?page_id=14

DHS. (n.d.). *http://www.dhs.gov/critical-infrastructure-sectors*. Retrieved 03 05, 2014, from Department of Homeland Security: http://www.dhs.gov/critical-infrastructure-sectors

Dodge R.C. Jr., H. B. (2009). Standards-Based Cyber Ecercises. *2009 International Conference on Availability, Reliability and Security*, 738-743.

Dodge R.C. Jr., R. D. (2003). Organization and Training of a Cyber Security Team. *2003 IEEE*, 4311-4316.

Dodge R.C. Jr., R. D. (2004). Organized Cyber Defense Competitions. *Proceedings of the IEEE International Conference on Advanced Learning Technologies*.

Dorene L. Kewley, J. L. (2014, February 13). *Observations on the effects of defense in depth on adversary behavior in cyber warfare.* Retrieved from bbn.com: http://www.bbn.com/resources/pdf/USMA_IEEE02.pdf

Edmondson, A. (1999). Psychological Safety and Learning Behavior in work Teams. *Administrative Science Quarterly Vol 44*, 350-383.

Felder R.M., B. R. (2003). Learn By doing. *Chemical Engineering Education*, 282-283.

Felder, R. a. (2003). *Learn by doing.* Chem. Engr Education.

Frank Stajano, P. W. (2011). Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM vol 54*, 70-75.

Guard, U. S. (2014, March 18). *Situational Awareness.* Retrieved from uscg.mil: http://www.uscg.mil/auxiliary/training/tct/chap5.pdf

Halevi, T., Lewis, J., & Memon, N. (2013, January 21). *Phishing, Personality Traits and Facebook.* Retrieved from arxiv.org: http://arxiv.org/pdf/1301.7643v2.pdf

Hoffman L.J., R. T. (2005). Exploring a National Cybersecurity Exercise for Universitites. *IEEE Security & Privacy* (pp. 27-33). IEEE Computer Society.

Holbrook, M., Sheng, S., Cranor, L., Downs, J., & Kumaraguru, P. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *CHI 2010 [electronic resource]; we are CHI; the 28th Annual CHI Conference on Human Factors in Computing Systems; conference proceedings & extende*, 373-382.

Hong, J. (2012, January NA). The state of phishing attacks. *Communications of the ACM*, pp. 74-81.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2014, January 16). *http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.* Retrieved from lockheedmartin.com: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

ICS2 CISSP information. (n.d.). Retrieved 03 06, 2014, from ICS2: https://www.isc2.org/uploadedFiles/Credentials_and_Certification/CISSP/CISSP-Information.pdf

ISO. (n.d.). Retrieved 03 05, 2014, from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

J., W. (2005). A Real-Time Information Warfare Exercise on a Virtual Netowrk. *Thirty-Sixth SIGCSE Technical Symposium*, 86-90.

Jakobsson, M. (2005). Modeling and Preventing Phishing Attacks. *Financial Cryptography (Vol 5)*.

Kerr, S. (1975). On the Folly of Rewarding A, While Hoping for B. *Academy of Management Journal Volume 18 Number 4*, 769-783.

Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development.* Englewood Cliffs, N.J.: Prentice-Hall, Inc.,.

Kotter, J. (2014, March 2014). *kotterinternational.com*. Retrieved from The 8-step process for leading change: http://www.kotterinternational.com/our-principles/changesteps/changesteps

Labs, K. (2013, January 21). *Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year*. Retrieved from kaspersky.com: http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year

Lacovos Kirlappos, M. A. (2014, February 20). *Security education against phishing: A modes proposal for a major re-think.* Retrieved from discovery.ucl.ac.uk: http://discovery.ucl.ac.uk/1353958/1/Kirlappos_Security_2012.pdf

Longshore, D. (1998). Self-Control and Criminal Opportunity: A Prospective Test of the General Theory of Crime. *Social Problems*, 102-113.

M.S., A. (2006). the Cyber Defense Laboratory: A Framework for Information Security Education. *Proceedings of the 2006 IEEE*, 55-60.

M.S., A. (2006). The CyberDefense Laboratory: A Framework for information Security Education. *Proceedings of the 2006 IEEE*, 55-60.

McCumber, C. J. (1991). INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL. *14th National Computer Security Conference* (p. unknown). unknown: Illinois Institute of Technology.

Morreale P., K. S. (2009). Methodology for successful undergraduate recruiting in computer science at comprehensive public universities. *40th ACM Technical Symposium on Computer Science Education*, (pp. 91-95).

Mullins B.E., L. T. (2007). How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. *IEEE Security & Privacy* (pp. 40-49). IEEE Computer Society.

P., B. (2006). Behaviorism, Constructivism, and Socratic Pedagogy. *Educationla Philosophy and Theory*, 713-722.

Patriciu V.V., F. A. (n.d.). Guide for Designing Cyber Security Exercises. *Recent Advances in E-activities, Information Security and Privacy*, 172-177.

Ponnurangam Kumaraguru, J. C. (2009). *School of Phish: A Real-Word Evaluation of Anti-Phishing Training.* Pittsburgh, PA: Carnegie Mellon University.

Ram Avtar, B. V. (2011). Data Shield Algorithm (DSA) for Security against Phishing Attacks. *An International Journal of Engineering Sciences*, 221-232.

Region, T. G. (2008). *AN OVERVIEW OF INFORMATION .* Hong Kong: Government of Hong Kong.

Reyes, C. (2014, March 6). *What makes a good security policy ans why is one necessary.* Retrieved from giac.org: http://www.giac.org/paper/gsec/1691/good-security-policy-necessary/103074

Rosenberg, T. a. (2006). Taking the network on the road: Portable network solutions for computer security educatiors. *Journal of Education Resource computing*, 1-13.

Rursch J.A., L. A. (2010). IT-Adventures: A program to Spark IT Interest in High School Studenets Using Inquiry -Based Learning with Cyber Defense, Game Design, and Robotics. *IEEE Transactions on Education* , 71-79.

Schepens W.J., J. J. (2003). Architecture of a Cyber Defense Competition. West Point , New York, USA.

Schepens W.J., R. D. (2001). *The Cyber Defense Exercise: An Evaluation of the Effectivenes of Information Assurance Education.* West Point: US Military Academy.

Schepens W.J., R. D. (2001). *the Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education.* Colorado Springs: US Air Force Academy.

Schneier, B. (1999). Attack Trees: Modeling Securtiy Threats. *Dr. Dobb's Journal*.

Schweitzer D., F. S. (n.d.). *A Hybrid Approach to Teaching Information Warefare.* Colorado Springs: US Air force Academy.

Small, P. E. (2011, February 13). *Defense in Depth: An Impractical Stragtegy for a Cyber World.* Retrieved from sans.org: https://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896

Team, T. A. (2014, February 20). *Spear-Phishing Email: Most Favored APT Attack Bait.* Retrieved from trendmicro.com: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Thornburgh, N. (2014, February 27). *Inside the Chinese Hack Attack*. Retrieved from time.com: http://content.time.com/time/nation/article/0,8599,1098371,00.html

V., L. (2004, Fall). Database Integration and Graphical User Interface for Cyber Defense Scoring System. Sacramento, California, USA.

Walter R. Nunn, D. V.-C. (1982). Technical Note - Analysis of a Layered Defense Model. *Operations Research 30(3)*, 595-599.

Welch D., R. D. (2001). *Trial-By-Fire in Informaiton Assurance Education.* West Point: US Military Academy.

Welch D., R. D. (2002). Training for Information Assurance. *2002 IEEE*, 30-37.

West, R. (2008). The Pshychology of Security. *Communications of the ACM Vol 51 No. 4*, 34-40.

White G. B., W. D. (2004). The Collegiate Cyber Defense Competition. *9th Colloquium for Information Systems Security Education.* Atlanta: Georgia Institute of Technology.

Zhang, W. (2012). How Could I Fall for That? Exploring Phishing Victimization with the Heuristic-Systematic Model. *System Science (HICSS), 2012 45th Hawaii International Conference on* , 2374 - 2380 .

Appendix

Table 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NUMBER	NIST SP 800-53 CONTROLS
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-7	Unsuccessful Login Attempts
AC-8	System Use Notification
AC-9	Previous Logon (Access)

	Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-12	Withdrawn
AC-13	Withdrawn
AC-14	Permitted Actions without Identification or Authentication
AC-15	Withdrawn
AC-16	Security Attributes
AC-17	Remote Access
AC-18	Wireless Access
AC-19	Access Control for Mobile Devices
AC-20	Use of External Information Systems
AC-21	User-Based Collaboration and Information Sharing
AC-22	Publicly Accessible Content
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AT-3	Security Training
AT-4	Security Training Records
AT-5	Contacts with Security Groups and Associations
AU-1	Audit and Accountability Policy and Procedures
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
AU-13	Monitoring for Information

	Disclosure
AU-14	Session Audit
CA-1	Security Assessment and Authorization Policies and Procedures
CA-2	Security Assessments
CA-3	Information System Connections
CA-4	Withdrawn
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CA-7	Continuous Monitoring
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-5	Access Restrictions for Change
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing and Exercises
CP-5	Withdrawn
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
IA-1	Identification and Authentication Policy and Procedures
IA-2	Identification and Authentication (Organizational Users)

IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing and Exercises
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance
IR-8	Incident Response Plan
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Non-Local Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
MP-1	Media Protection Policy and Procedures
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization
PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-4	Access Control for Transmission Medium
PE-5	Access Control for Output Devices
PE-6	Monitoring Physical Access

PE-7	Visitor Control
PE-8	Access Records
PE-9	Power Equipment and Power Cabling
PE-10	Emergency Shutoff
PE-11	Emergency Power
PE-12	Emergency Lighting
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection
PE-16	Delivery and Removal
PE-17	Alternate Work Site
PE-18	Location of Information System Components
PE-19	Information Leakage
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
PL-3	Withdrawn
PL-4	Rules of Behavior
PL-5	Privacy Impact Assessment
PL-6	Security-Related Activity Planning
PS-1	Personnel Security Policy and Procedures
PS-2	Position Categorization
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
RA-3	Risk Assessment
RA-4	Withdrawn
RA-5	Vulnerability Scanning
SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	Life Cycle Support

SA-4	Acquisitions
SA-5	Information System Documentation
SA-6	Software Usage Restrictions
SA-7	User-Installed Software
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
SA-12	Supply Chain Protections
SA-13	Trustworthiness
SA-14	Critical Information System Components
SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information In Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Priority
SC-7	Boundary Protection
SC-8	Transmission Integrity
SC-9	Transmission Confidentiality
SC-10	Network Disconnect
SC-11	Trusted Path
SC-12	Cryptographic Key Establishment and Management
SC-13	Use of Cryptography
SC-14	Public Access Protections
SC-15	Collaborative Computing Devices
SC-16	Transmission of Security Attributes
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name /Address Resolution Service (Authoritative Source)
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)

SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity
SC-24	Fail in Known State
SC-25	Thin Nodes
SC-26	Honeypots
SC-27	Operating System-Independent Applications
SC-28	Protection of Information at Rest
SC-29	Heterogeneity
SC-30	Virtualization Techniques
SC-31	Covert Channel Analysis
SC-32	Information System Partitioning
SC-33	Transmission Preparation Integrity
SC-34	Non-Modifiable Executable Programs
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Functionality Verification
SI-7	Software and Information Integrity
SI-8	Spam Protection
SI-9	Information Input Restrictions
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Output Handling and Retention
SI-13	Predictable Failure Prevention
PM-1	Information Security Program Plan
PM-2	Senior Information Security Officer
PM-3	Information Security Resources
PM-4	Plan of Action and Milestones Process
PM-5	Information System Inventory
PM-6	Information Security Measures of Performance
PM-7	Enterprise Architecture
PM-8	Critical Infrastructure Plan

PM-9	Risk Management Strategy
PM-10	Security Authorization Process
PM-11	Mission/Business Process Definition

Table 2: ISO/IEC 27001 Controls

ISO/IEC 27001 (Annex A) CONTROLS
A.5 Security Policy
A.5.1 Information security policy
A.5.1.1 Information security policy document
A.5.1.2 Review of the information security policy
A.6 Organization of information security
A.6.1 Internal
A.6.1.1 Management commitment to information security
A.6.1.2 Information security coordination
A.6.1.3 Allocation of information security responsibilities
A.6.1.4 Authorization process for information processing facilities
A.6.1.5 Confidentiality agreements
A.6.1.6 Contact with authorities
A.6.1.7 Contact with special interest groups
A.6.1.8 Independent review of information security
A.6.2 External Parties
A.6.2.1 Identification of risks related to external parties
A.6.2.2 Addressing security when dealing with customers
A.6.2.3 Addressing security in third party agreements
A.7 Asset Management
A.7.1 Responsibility for assets
A.7.1.1 Inventory of assets
A.7.1.2 Ownership of assets
A.7.1.3 Acceptable use of assets
A.7.2 Information Classification
A.7.2.1 Classification Guidelines
A.7.2.2 Information labeling and handling
A.8 Human Resources Security
A.8.1 Prior to Employment
A.8.1.1 Roles and Responsibilities
A.8.1.2 Screening
A.8.1.3 Terms and conditions of employment
A.8.2 During employment
A.8.2.1 Management responsibilities
A.8.2.2 Awareness, education, and training
A.8.2.3 Disciplinary process
A.8.3 Termination or change of employment
A.8.3.1 Termination responsibilities
A.8.3.2 Return of assets

A.8.3.3 Removal of access rights
A.9 Physical and environmental security
A.9.1 Secure areas
A.9.1.1 Physical security perimeter
A.9.1.2 Physical entry controls
A.9.1.3 Securing offices, rooms, facilities
A.9.1.4 Protecting against external and environmental threats
A.9.1.5 Working in secure areas
A.9.1.6 Public access, delivery and loading areas
A.9.2 Equipment security
A.9.2.1 Equipment siting and protection
A.9.2.2 Supporting utilities
A.9.2.3 Cabling security
A.9.2.4 Equipment maintenance
A.9.2.5 Security of equipment off-premises
A.9.2.6 Secure disposal or reuse of equipment
A.9.2.7 Removal of property
A.10 Communications and operations management
A.10.1 Operational procedures and responsibilities
A.10.1.1 Documented operating procedures
A.10.1.2 Change management
A.10.1.3 Segregation of duties
A.10.1.4 Separation of development, test and operational facilities
A.10.2 Third-party service delivery management
A.10.2.1 Service delivery
A.10.2.2 Monitoring and review of third-party services
A.10.2.3 Managing changes to third-party services
A.10.3 System planning and acceptance
A.10.3.1 Capacity management
A.10.3.2 System acceptance
A.10.4 Protection against malicious and mobile code
A.10.4.1 Controls against malicious code
A.10.4.2 Controls against mobile code
A.10.5 Backup
A.10.5.1 Information backup
A.10.6 Network security management
A.10.6.1 Network controls
A.10.6.2 Security of network services
A.10.7 Media handling
A.10.7.1 Management of removable media
A.10.7.2 Disposal of media

A.10.7.3 Information handling procedures
A.10.7.4 Security of system documentation
A.10.8 Exchange of information
A.10.8.1 Information exchange policies and procedures
A.10.8.2 Exchange agreements
A.10.8.3 Physical media in transit
A.10.8.4 Electronic messaging
A.10.8.5 Business information systems
A.10.9 Electronic commerce services
A.10.9.1 Electronic commerce
A.10.9.2 Online transactions
A.10.9.3 Publicly available information
A.10.10 Monitoring
A.10.10.1 Audit logging
A.10.10.2 Monitoring system use
A.10.10.3 Protection of log information
A.10.10.4 Administrator and operator logs
A.10.10.5 Fault logging
A.10.10.6 Clock synchronization
A.11 Access Control
A.11.1 Business requirement for access control
A.11.1.1 Access control policy
A.11.2 User access management
A.11.2.1 User registration
A.11.2.2 Privilege management
A.11.2.3 User password management
A.11.2.4 Review of user access rights
A 11.3 User responsibilities
A.11.3.1 Password use
A.11.3.2 Unattended user equipment
A.11.3.3 Clear desk and clear screen policy
A.11.4 Network access control
A.11.4.1 Policy on use of network services
A.11.4.2 User authentication for external connections
A.11.4.3 Equipment identification in networks
A.11.4.4 Remote diagnostic and configuration port protection
A.11.4.5 Segregation in networks
A.11.4.6 Network connection control
A.11.4.7 Network routing control
A 11.5 Operating system access control
A.11.5.1 Secure log-on procedures

A.11.5.2 User identification and authentication
A.11.5.3 Password management system
A.11.5.4 Use of system utilities
A.11.5.5 Session time-out
A.11.5.6 Limitation of connection time
A.11.6 Application and information access control
A.11.6.1 Information access restriction
A.11.6.2 Sensitive system isolation
A.11.7 Mobile computing and teleworking
A.11.7.1 Mobile computing and communications
A.11.7.2 Teleworking
A.12 Information systems acquisition, development and maintenance
A.12.1 Security requirements of information systems
A.12.1.1 Security requirements analysis and specification
A.12.2 Correct processing in applications
A.12.2.1 Input data validation
A.12.2.2 Control of internal processing
A.12.2.3 Message integrity
A.12.2.4 Output data validation
A.12.3 Cryptographic controls
A.12.3.1 Policy on the use of cryptographic controls
A.12.3.2 Key management
A.12.4 Security of system files
A.12.4.1 Control of operational software
A.12.4.2 Protection of system test data
A.12.4.3 Access control to program source code
A.12.5 Security in development and support processes
A.12.5.1 Change control procedures
A.12.5.2 Technical review of applications after operating system changes
A.12.5.3 Restrictions on changes to software packages
A.12.5.4 Information leakage
A.12.5.5 Outsourced software development
A.12.6 Technical Vulnerability Management
A.12.6.1 Control of technical vulnerabilities
A.13 Information security incident management
A.13.1 Reporting information security events and weaknesses
A.13.1.1 Reporting information security events
A.13.1.2 Reporting security weaknesses
A.13.2 Management of information security incidents and improvements
A.13.2.1 Responsibilities and procedures

A.13.2.2 Learning from information security incidents
A.13.2.3 Collection of evidence
A.14 Business continuity management
A.14.1 Information security aspects of business continuity management
A.14.1.1 Including information security in the business continuity management process
A.14.1.2 Business continuity and risk assessment
A.14.1.3 Developing and implementing continuity plans including information security
A.14.1.4 Business continuity planning framework
A.14.1.5 Testing, maintaining and reassessing business continuity plans
A.15 Compliance
A.15.1 Compliance with legal requirements
A.15.1.1 Identification of applicable legislation
A.15.1.2 Intellectual property rights (IPR)
A.15.1.3 Protection of organizational records
A.15.1.4 Data protection and privacy of personal information
A.15.1.5 Prevention of misuse of information processing facilities
A.15.1.6 Regulation of cryptographic controls
A.15.2 Compliance with security policies and standards, and technical compliance
A.15.2.1 Compliance with security policies and standards
A.15.2.2 Technical compliance checking
A.15.3 Information systems audit considerations
A.15.3.1 Information systems audit controls
A.15.3.2 Protection of information systems audit tools

Table 3: Standards Cross Referenced to Domains

	CISSP	NIST	ISO	COSO	HIPAA	COBIT
Access control	X	X	X		X	
Telecommunications and network security	X					
Information security governance and risk management	X	X	X	X	X	
Software development security	X					X
Cryptography	X					
Security architecture and design	X					X
Operations security	X					
Business continuity and disaster recovery planning	X					
Legal, regulations, investigations and compliance	X		X	X		X
Physical (environmental) security	X	X	X			
Awareness and Training		X			X	X
Audit and Accountability		X	X		X	X
Security Assessment and Authorization		X				
Configuration Management		X			X	
Contingency Planning		X	X			
Identification and Authentication		X				
Incident Response		X	X			X
Maintenance		X	X			
Media Protection		X				
Planning		X				X
Personnel Security		X	X	X	X	X
System and Services Acquisition		X				
System and Communications Protection		X	X	X		X
Program Management		X				
Transmission Security					X	
PO1 Define a Strategic IT Plan						X
PO3 Determine Technological Direction						X
PO4 Define the IT Organization and Relationships						X
PO5 Manage the IT Investment						X
Acquisition & Implementation						X

Identify Automated Solutions						X
Develop and Maintain Procedures						X
Install and Accredit Systems						X
Manage Changes						X
Delivery and Support						X
Define and Manage Service Levels						X
Manage Third Party Services						X
Manage Performance and Capacity						X
Ensure Continuous Service						X
Ensure Systems Security						X
Indentify and Allocate Costs						X
Assist and Advise Customers						X
Manage Data						X

Table 4: DHS Domain Cross-Reference

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, 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.	ID.AM-1: Physical devices and systems within the organization are inventoried	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification,	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1

		criticality, and business value	· NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): 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.	ID.BE-1: The organization's role in the supply chain is identified and communicated	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Governance (ID.GV): The	ID.GV-1: Organizational	· COBIT 5 APO01.03, EDM01.01, EDM01.02

	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 policy is established	· ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
		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 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · 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
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5

		ID.RA-3: Threats, both internal and external, are identified and documented	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		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
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 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	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	Access Control (PR.AC): Access to assets and	PR.AC-1: Identities and credentials are managed for	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03

	associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	authorized devices and users	· ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013

			A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013

			A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · 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 · NIST SP 800-53 Rev. 4 SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2

			· ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11,

	systems and assets.		SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Protection	· COBIT 5 APO11.06,

		processes are continuously improved	DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance	PR.MA-1:	· COBIT 5 BAI09.03

	(PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7,

			4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	· CCS CSC 7 · COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of	· COBIT 5 APO12.06

		events is determined	· NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Unauthorized mobile code is detected	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: External service provider	· COBIT 5 APO07.06 · ISO/IEC 27001:2013

		activity is monitored to detect potential cybersecurity events	A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		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
		DE.CM-8: Vulnerability scans are performed	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9

		appropriate parties	· ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8,

			PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		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
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Forensics are performed	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are	RS.MI-1: Incidents are contained	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR

	performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.		5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and	RC.IM-1: Recovery plans incorporate lessons learned	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

	processes are improved by incorporating lessons learned into future activities.	RC.IM-2: Recovery strategies are updated	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	· COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	· COBIT 5 MEA03.02
		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

Table 5: Standard to Controls Cross Referencing

MAPPING NIST SP 800-53 TO ISO/IEC 27001 (ANNEX A)

NUMBER	NIST SP 800-53 CONTROLS	ISO/IEC 27001 (Annex A) CONTROLS
AC-1	Access Control Policy and Procedures	A5.1.1, A5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A10.1.1, A.10.8.1, A.11.1.1, A.11.2.1, A11.2.2, A11.4.1, A.11.7.1, A.11.7.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A15.2.1
AC-3	Access Enforcement	A.10.8.1 A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.2
AC-4	Information Flow Enforcement	A.10.6.1, A.10.8.1, A.11.4.5, A.11.4.7, A.11.7.2, A.12.4.2, A.12.5.4
AC-5	Separation of Duties	A.6.1.3, A.8.1.1, A.10.1.3, A.11.1.1, A.11.4.1
AC-6	Least Privilege	A.6.1.3, A.8.1.1, A.11.1.1, A.11.2.2, A.11.4.1, A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Login Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.8.1.1, A.11.5.1, A.15.1.5
AC-9	Previous Logon (Access) Notification	A.11.5.1
AC-10	Concurrent Session Control	A.11.5.1
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	Withdrawn	---
AC-13	Withdrawn	---
AC-14	Permitted Actions without Identification or Authentication	A.11.6.1
AC-15	Withdrawn	---
AC-16	Security Attributes	A.7.2.2
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2

AC-18	Wireless Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-19	Access Control for Mobile Devices	A.10.4.1, A.11.1.1, A.11.4.3, A.11.7.1
AC-20	Use of External Information Systems	A.7.1.3, A.8.1.1, A.8.1.3, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2
AC-21	User-Based Collaboration and Information Sharing	A.11.2.1, A.11.2.2
AC-22	Publicly Accessible Content	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
AT-2	Security Awareness	A.6.2.2, A.8.1.1, A.8.2.2, A.9.1.5, A.10.4.1
AT-3	Security Training	A.8.1.1, A.8.2.2, A.9.1.5
AT-4	Security Training Records	None
AT-5	Contacts with Security Groups and Associations	A.6.1.7
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.10.2, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Auditable Events	A.10.10.1, A.10.10.4, A.10.10.5, A.15.3.1
AU-3	Content of Audit Records	A.10.10.1
AU-4	Audit Storage Capacity	A.10.10.1, A.10.3.1
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.1
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation	A.10.10.2
AU-8	Time Stamps	A.10.10.1, A.10.10.6
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-10	Non-repudiation	A.10.9.1, A.12.2.3
AU-11	Audit Record Retention	A.10.10.1, A.10.10.2, A.15.1.3
AU-12	Audit Generation	A.10.10.1, A.10.10.4, A.10.10.5
AU-13	Monitoring for Information Disclosure	None

AU-14	Session Audit	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.6.1.4, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.10.3.2, A.15.2.1, A.15.2.2
CA-3	Information System Connections	A.6.2.1, A.6.2.3, A.10.6.1, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	Withdrawn	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.15.2.1, A.15.2.2
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.1.2, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.12.4.1, A.10.1.4
CM-3	Configuration Change Control	A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.11.1.1, A.11.6.1, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	None
CM-7	Least Functionality	None
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.8.1.1, A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.10.1.1, A.10.1.2, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1

CP-2	Contingency Plan	A.6.1.2, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training	A.8.2.2, A.9.1.4, A.14.1.3
CP-4	Contingency Plan Testing and Exercises	A.6.1.2, A.9.1.4, A.14.1.1, A.14.1.3, A.14.1.4, A.14.1.5
CP-5	Withdrawn	---
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services	A.9.1.4, A.10.6.1, A.14.1.3
CP-9	Information System Backup	A.9.1.4, A.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution	A.9.1.4, A.14.1.3
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.11.2.1, A.15.1.1, A.15.2.1
IA-2	Identification and Authentication (Organizational Users)	A.11.3.2, A.11.5.1, A.11.5.2, A.11.5.3
IA-3	Device Identification and Authentication	A.11.4.3
IA-4	Identifier Management	A.11.5.2
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback	A.11.5.1
IA-7	Cryptographic Module Authentication	A.12.3.1, A.15.1.1, A.15.1.6, A.15.2.1
IA-8	Identification and Authentication (Non-Organizational Users)	A.10.9.1, A.11.4.2, A.11.5.1, A.11.5.2
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training	A.8.2.2
IR-3	Incident Response Testing and Exercises	None
IR-4	Incident Handling	A.6.1.2, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	None

MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.2.4, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance	A.9.2.4
MA-3	Maintenance Tools	A.9.2.4, A.11.4.4
MA-4	Non-Local Maintenance	A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel	A.9.2.4, A.12.4.3
MA-6	Timely Maintenance	A.9.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.10.7.2, A.10.7.3, A.11.1.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access	A.7.2.2, A.10.7.1, A.10.7.3
MP-3	Media Marking	A.7.2.2, A.10.7.1, A.10.7.3
MP-4	Media Storage	A.10.7.1, A.10.7.3, A.10.7.4, A.15.1.3
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.7.3, A.10.8.3
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2, A.10.7.3
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.9.2.1, A.9.2.2, A.10.1.1, A.11.1.1, A.11.2.1, A.11.2.2, A.15.1.1, A.15.2.1
PE-2	Physical Access Authorizations	A.9.1.5, A.11.2.1, A.11.2.2, A.11.2.4
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.5, A.9.1.6, A.11.3.2, A.11.4.4
PE-4	Access Control for Transmission Medium	A.9.1.3, A.9.1.5, A.9.2.3
PE-5	Access Control for Output Devices	A.9.1.2, A.9.1.3, A.10.6.1, A.11.3.2
PE-6	Monitoring Physical Access	A.9.1.2, A.9.1.5, A.10.10.2
PE-7	Visitor Control	A.9.1.2, A.9.1.5, A.9.1.6
PE-8	Access Records	A.9.1.5, A.10.10.2, A.15.2.1
PE-9	Power Equipment and Power Cabling	A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff	A.9.1.4
PE-11	Emergency Power	A.9.1.4, A.9.2.2

PE-12	Emergency Lighting	A.9.2.2
PE-13	Fire Protection	A.9.1.4
PE-14	Temperature and Humidity Controls	A.9.2.2
PE-15	Water Damage Protection	A.9.1.4
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7, A.10.7.1
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2
PE-18	Location of Information System Components	A.9.2.1, A.11.3.2
PE-19	Information Leakage	A.12.5.4
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PL-2	System Security Plan	None
PL-3	Withdrawn	---
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.12.4.1, A.13.1.2, A.15.1.5
PL-5	Privacy Impact Assessment	A.15.1.4
PL-6	Security-Related Activity Planning	A.6.1.2, A.15.3.1
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PS-2	Position Categorization	A.8.1.1
PS-3	Personnel Screening	A.8.1.2
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements	A.6.1.5, A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
PS-7	Third-Party Personnel Security	A.6.2.3, A.8.1.1, A.8.2.1, A.8.1.3
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.2, A.15.1.1, A.15.2.1
RA-2	Security Categorization	A.7.2.1, A.14.1.2
RA-3	Risk Assessment	A.6.2.1, A.10.2.3, A.12.6.1, A.14.1.2
RA-4	Withdrawn	---

RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.6.2.1, A.8.1.1, A.10.1.1, A.12.1.1, A.12.5.5, A.15.1.1, A.15.2.1
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1
SA-3	Life Cycle Support	A.12.1.1
SA-4	Acquisitions	A.12.1.1, A.12.5.5
SA-5	Information System Documentation	A.10.7.4, A.15.1.3
SA-6	Software Usage Restrictions	A.12.4.1, A.12.5.5, A.15.1.2
SA-7	User-Installed Software	A.12.4.1, A.12.5.5, A.15.1.5
SA-8	Security Engineering Principles	A.10.4.1, A.10.4.2, A.11.4.5, A.12.5.5
SA-9	External Information System Services	A.6.1.5, A.6.2.1, A.6.2.3, A.8.1.1, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5
SA-10	Developer Configuration Management	A.12.4.3, A.12.5.1, A.12.5.5
SA-11	Developer Security Testing	A.10.3.2, A.12.5.5
SA-12	Supply Chain Protections	A.12.5.5
SA-13	Trustworthiness	A.12.5.5
SA-14	Critical Information System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SC-2	Application Partitioning	A.10.4.1, A.10.4.2
SC-3	Security Function Isolation	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	A.10.3.1
SC-6	Resource Priority	None
SC-7	Boundary Protection	A.6.2.1, A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.5, A.11.4.6
SC-8	Transmission Integrity	A.10.4.2, A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.2.3,

		A.12.3.1
SC-9	Transmission Confidentiality	A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.3.1
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.1, A.11.5.5
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.12.3.2
SC-13	Use of Cryptography	A.12.3.1, A.15.1.6
SC-14	Public Access Protections	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2, A.10.9.3
SC-15	Collaborative Computing Devices	None
SC-16	Transmission of Security Attributes	A.7.2.2, A.10.8.1
SC-17	Public Key Infrastructure Certificates	A.12.3.2
SC-18	Mobile Code	A.10.4.2
SC-19	Voice Over Internet Protocol	A.10.6.1
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	A.10.6.1
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1
SC-23	Session Authenticity	A.10.6.1
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Operating System-Independent Applications	None
SC-28	Protection of Information at Rest	None
SC-29	Heterogeneity	None
SC-30	Virtualization Techniques	None
SC-31	Covert Channel Analysis	None
SC-32	Information System Partitioning	None
SC-33	Transmission Preparation Integrity	None
SC-34	Non-Modifiable Executable Programs	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation	A.10.10.5, A.12.5.2, A.12.6.1, A.13.1.2

SI-3	Malicious Code Protection	A.10.4.1
SI-4	Information System Monitoring	A.10.10.2, A.13.1.1, A.13.1.2
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.12.6.1, A.13.1.1, A.13.1.2
SI-6	Security Functionality Verification	None
SI-7	Software and Information Integrity	A.10.4.1, A.12.2.2, A.12.2.3
SI-8	Spam Protection	None
SI-9	Information Input Restrictions	A.10.8.1, A.11.1.1, A.11.2.2, A.12.2.2
SI-10	Information Input Validation	A.12.2.1, A.12.2.2
SI-11	Error Handling	None
SI-12	Information Output Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4, A.15.2.1
SI-13	Predictable Failure Prevention	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.8.1.1, A.15.1.1, A.15.2.1
PM-2	Senior Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	A.7.1.1, A.7.1.2
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	A.6.2.1, A.14.1.2
PM-10	Security Authorization Process	A.6.1.4
PM-11	Mission/Business Process Definition	None

Table 6:Mapping ISO/IEC 27001 to NIST SP 800-53

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.5 Security Policy	
A.5.1 Information security policy	
A.5.1.1 Information security policy document	XX-1 controls
A.5.1.2 Review of the information security policy	XX-1 controls
A.6 Organization of information security	
C	
A.6.1.1 Management commitment to information security	XX-1 controls, PM-2; SP 800-39, SP 800-37
A.6.1.2 Information security coordination	CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37
A.6.1.4 Authorization process for information processing facilities	CA-1, CA-6, PM-10; SP 800-37
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9
A.6.1.6 Contact with authorities	Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37
A.6.1.7 Contact with special interest groups	AT-5
A.6.1.8 Independent review of information security	CA-2, CA-7; SP 800-39, SP 800-37
A.6.2 External Parties	
A.6.2.1 Identification of risks related to external parties	CA-3, PM-9, RA-3, SA-1, SA-9, SC-7
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, PL-4
A.6.2.3 Addressing security in third party agreements	CA-3, PS-7, SA-9
A.7 Asset Management	
A.7.1 Responsibility for assets	
A.7.1.1 Inventory of assets	CM-8, CM-9, PM-5
A.7.1.2 Ownership of assets	CM-8, CM-9, PM-5
A.7.1.3 Acceptable use of assets	AC-20, PL-4

A.7.2 Information Classification	
A.7.2.1 Classification Guidelines	RA-2
A.7.2.2 Information labeling and handling	AC-16, MP-2, MP-3, SC-16
A.8 Human Resources Security	
A.8.1 Prior to Employment	
A.8.1.1 Roles and Responsibilities	XX-1 controls, AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
A.8.1.2 Screening	PS-3
A.8.1.3 Terms and conditions of employment	AC-20, PL-4, PS-6, PS-7
A.8.2 During employment	
A.8.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.8.2.2 Awareness, education, and training	AT-2, AT-3, IR-2
A.8.2.3 Disciplinary process	PS-8
A.8.3 Termination or change of employment	
A.8.3.1 Termination responsibilities	PS-4, PS-5
A.8.3.2 Return of assets	PS-4, PS-5
A.8.3.3 Removal of access rights	AC-2, PS-4, PS-5
A.9 Physical and environmental security	
A.9.1 Secure areas	
A.9.1.1 Physical security perimeter	PE-3
A.9.1.2 Physical entry controls	PE-3, PE-5, PE-6, PE-7
A.9.1.3 Securing offices, rooms, facilities	PE-3, PE-4, PE-5
A.9.1.4 Protecting against external and environmental threats	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15
A.9.1.5 Working in secure areas	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8
A.9.1.6 Public access, delivery and loading areas	PE-3 , PE-7, PE-16
A.9.2 Equipment security	
A.9.2.1 Equipment siting and protection	PE-1, PE-18
A.9.2.2 Supporting utilities	PE-1, PE-9, PE-11, PE-12, PE-14
A.9.2.3 Cabling security	PE-4, PE-9
A.9.2.4 Equipment maintenance	MA Family

A.9.2.5 Security of equipment off-premises	MP-5, PE-17
A.9.2.6 Secure disposal or reuse of equipment	MP-6
A.9.2.7 Removal of property	MP-5, PE-16
A.10 Communications and operations management	
A.10.1 Operational procedures and responsibilities	
A.10.1.1 Documented operating procedures	XX-1 controls, CM-9
A.10.1.2 Change management	CM-1, CM-3, CM-4, CM-5, CM-9
A.10.1.3 Segregation of duties	AC-5
A.10.1.4 Separation of development, test and operational facilities	CM-2
A.10.2 Third-party service delivery management	
A.10.2.1 Service delivery	SA-9
A.10.2.2 Monitoring and review of third-party services	SA-9
A.10.2.3 Managing changes to third-party services	RA-3, SA-9
A.10.3 System planning and acceptance	
A.10.3.1 Capacity management	AU-4, AU-5, CP-2, SA-2, SC-5
A.10.3.2 System acceptance	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11
A.10.4 Protection against malicious and mobile code	
A.10.4.1 Controls against malicious code	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
A.10.4.2 Controls against mobile code	SA-8, SC-2, SC-3, SC-7, SC-14, SC-8, SC-18
A.10.5 Backup	
A.10.5.1 Information backup	CP-9
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	SA-9, SC-8, SC-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16

A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
A.10.9.2 Online transactions	SC-3, SC-7, SC-8, SC-9, SC-14
A.10.9.3 Publicly available information	SC-14
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
A.10.10.2 Monitoring system use	AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4
A.10.10.3 Protection of log information	AU-9
A.10.10.4 Administrator and operator logs	AU-2, AU-12
A.10.10.5 Fault logging	AU-2, AU-6, AU-12, SI-2
A.10.10.6 Clock synchronization	AU-8
A.11 Access Control	
A.11.1 Business requirement for access control	
A.11.1.1 Access control policy	AC-1, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1, SI-9
A.11.2 User access management	
A.11.2.1 User registration	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
A.11.2.2 Privilege management	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9
A.11.2.3 User password management	IA-5
A.11.2.4 Review of user access rights	AC-2, PE-2
A 11.3 User responsibilities	

A.11.3.1 Password use	IA-2, IA-5
A.11.3.2 Unattended user equipment	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10
A.11.3.3 Clear desk and clear screen policy	AC-11
A.11.4 Network access control	
A.11.4.1 Policy on use of network services	AC-1, AC-5, AC-6, AC-17, AC-18, AC-20
A.11.4.2 User authentication for external connections	AC-17, AC-18, AC-20, CA-3, IA-2, IA-8
A.11.4.3 Equipment identification in networks	AC-19, IA-3
A.11.4.4 Remote diagnostic and configuration port protection	AC-3, AC-6, AC-17, AC-18, PE-3, MA-3, MA-4
A.11.4.5 Segregation in networks	AC-4, SA-8, SC-7
A.11.4.6 Network connection control	AC-3, AC-6, AC-17, AC-18, SC-7
A.11.4.7 Network routing control	AC-4, AC-17, AC-18
A 11.5 Operating system access control	
A.11.5.1 Secure log-on procedures	AC-7, AC-8, AC-9, AC-10, IA-2, IA-6, IA-8, SC-10
A.11.5.2 User identification and authentication	IA-2, IA-4, IA-5, IA-8
A.11.5.3 Password management system	IA-2, IA-5
A.11.5.4 Use of system utilities	AC-3, AC-6
A.11.5.5 Session time-out	AC-11, SC-10
A.11.5.6 Limitation of connection time	None
A.11.6 Application and information access control	
A.11.6.1 Information access restriction	AC-3, AC-6, AC-14, CM-5
A.11.6.2 Sensitive system isolation	None; SP 800-39
A.11.7 Mobile computing and teleworking	
A.11.7.1 Mobile computing and communications	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6
A.11.7.2 Teleworking	AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6
A.12 Information systems acquisition, development and maintenance	
A.12.1 Security requirements of	

information systems	
A.12.1.1 Security requirements analysis and specification	SA-1, SA-3, SA-4
A.12.2 Correct processing in applications	
A.12.2.1 Input data validation	SI-10
A.12.2.2 Control of internal processing	SI-7, SI-9, SI-10
A.12.2.3 Message integrity	AU-10, SC-8, SI-7
A.12.2.4 Output data validation	None
A.12.3 Cryptographic controls	
A.12.3.1 Policy on the use of cryptographic controls	Multiple controls address cryptography (e.g., IA-7, SC-8, SC-9, SC-12, SC-13)
A.12.3.2 Key management	SC-12, SC-17
A.12.4 Security of system files	
A.12.4.1 Control of operational software	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, PL-4, SA-6, SA-7
A.12.4.2 Protection of system test data	Multiple controls; protection of test data not addressed separately in SP 800-53 (e.g., AC-3, AC-4)
A.12.4.3 Access control to program source code	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10
A.12.5 Security in development and support processes	
A.12.5.1 Change control procedures	CM-1, CM-3, CM-9, SA-10
A.12.5.2 Technical review of applications after operating system changes	CM-3, CM-4, CM-9, SI-2
A.12.5.3 Restrictions on changes to software packages	CM-3, CM-4, CM-5, CM-9
A.12.5.4 Information leakage	AC-4, PE-19
A.12.5.5 Outsourced software development	SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13
A.12.6 Technical Vulnerability Management	
A.12.6.1 Control of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.13 Information security incident management	
A.13.1 Reporting information security events and weaknesses	
A.13.1.1 Reporting information security events	AU-6, IR-1, IR-6, SI-4, SI-5

A.13.1.2 Reporting security weaknesses	PL-4, SI-2, SI-4, SI-5
A.13.2 Management of information security incidents and improvements	
A.13.2.1 Responsibilities and procedures	IR-1
A.13.2.2 Learning from information security incidents	IR-4
A.13.2.3 Collection of evidence	AU-9, IR-4
A.14 Business continuity management	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2, CP-4
A.14.1.2 Business continuity and risk assessment	CP-2, PM-9, RA Family
A.14.1.3 Developing and implementing continuity plans including information security	CP Family
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
A.15 Compliance	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls, IA-7
A.15.1.2 Intellectual property rights (IPR)	SA-6
A.15.1.3 Protection of organizational records	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	PL-5; SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, PL-4, PS-6, PS-8, SA-7
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and	

technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8, SI-12
A.15.2.2 Technical compliance checking	CA-2, CA-7, RA-5
A.15.3 Information systems audit considerations	
A.15.3.1 Information systems audit controls	AU-1, AU-2, PL-6
A.15.3.2 Protection of information systems audit tools	AU-9

SQL script to build Database

```
USE FoxThesis_dev

IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[DomainToControl]') AND type in (N'U'))
   DROP TABLE [dbo].[DomainToControl]
GO

CREATE TABLE dbo.DomainToControl (
DomainToControlID int IDENTITY (1,1) PRIMARY KEY,
DomainID int,
ControlMeasureID int
)
GO


IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[Injects]') AND type in (N'U'))
   DROP TABLE [dbo].[Injects]
GO


CREATE TABLE dbo.Injects (
InjectID int IDENTITY (1,1) PRIMARY KEY,
Name nvarchar(50),
[Description] nvarchar(max)
)
GO


IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[Standards]') AND type in (N'U'))
   DROP TABLE [dbo].[Standards]
GO

CREATE TABLE dbo.Standards (
StandardID int IDENTITY (1,1) Primary Key,
Name nvarchar(50)
)
GO


IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[Domains]') AND type in (N'U'))
   DROP TABLE [dbo].[Domains]
```

```
GO

CREATE TABLE dbo.Domains (
DomainID int IDENTITY (1,1) Primary Key,
Name nvarchar(50)
)
GO

IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[Controls]') AND type in (N'U'))
   DROP TABLE [dbo].[Controls]
GO

CREATE TABLE dbo.ControlMeasures(
        ControlMeasureID int IDENTITY(1,1) PRIMARY KEY,
        Name nvarchar(50)
)
GO

IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[ControlNames]') AND type in (N'U'))
   DROP TABLE [dbo].[ControlNames]
GO


CREATE TABLE dbo.ControlNames (
DomainToStandardID int IDENTITY (1,1) PRIMARY KEY,
ControlMeasureID int,
Number nvarchar(50)
)
GO

IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[InjectToDomain]') AND type in (N'U'))
   DROP TABLE [dbo].[InjectToDomain]
GO

CREATE TABLE dbo.InjectToDomain (
InjectToDomainID int IDENTITY (1,1) PRIMARY KEY,
InjectID int,
DomainID int
)
GO
```

```
IF  EXISTS (SELECT * FROM sys.objects WHERE object_id =
OBJECT_ID(N'[dbo].[DomainToStandard]') AND type in (N'U'))
   DROP TABLE [dbo].[DomainToStandard]
GO
CREATE TABLE dbo.DomainToStandard (
DomainToStandardID int IDENTITY (1,1) PRIMARY KEY,
DomainID INT,
StandardID INT,
Name nvarchar(50)
)
GO


ALTER TABLE [dbo].[DomainToControl] WITH CHECK ADD CONSTRAINT
[Controls_DomainToControl_FK1] FOREIGN KEY (
[ControlMeasureID]
)
REFERENCES [dbo].[ControlMeasures] (
[ControlMeasureID]
)
ALTER TABLE [dbo].[DomainToControl] WITH CHECK ADD CONSTRAINT
[Domains_DomainToControl_FK1] FOREIGN KEY (
[DomainID]
)
REFERENCES [dbo].[Domains] (
[DomainID]
)
GO

GO

GO

GO

GO

ALTER TABLE [dbo].[ControlNames] WITH CHECK ADD CONSTRAINT
[Controls_ControlNames_FK1] FOREIGN KEY (
[ControlMeasureID]
)
REFERENCES [dbo].[ControlMeasures] (
[ControlMeasureID]
)
ALTER TABLE [dbo].[ControlNames] WITH CHECK ADD CONSTRAINT
[DomainToStandard_ControlNames_FK1] FOREIGN KEY (
```

```
[DomainToStandardID]
)
REFERENCES [dbo].[DomainToStandard] (
[DomainToStandardID]
)
GO

ALTER TABLE [dbo].[InjectToDomain] WITH CHECK ADD CONSTRAINT
[Injects_InjectToDomain_FK1] FOREIGN KEY (
[InjectID]
)
REFERENCES [dbo].[Injects] (
[InjectID]
)
ALTER TABLE [dbo].[InjectToDomain] WITH CHECK ADD CONSTRAINT
[Domains_InjectToDomain_FK1] FOREIGN KEY (
[DomainID]
)
REFERENCES [dbo].[Domains] (
[DomainID]
)
GO

ALTER TABLE [dbo].[DomainToStandard] WITH CHECK ADD CONSTRAINT
[Domains_DomainToStandard_FK1] FOREIGN KEY (
[DomainID]
)
REFERENCES [dbo].[Domains] (
[DomainID]
)
ALTER TABLE [dbo].[DomainToStandard] WITH CHECK ADD CONSTRAINT
[Standards_DomainToStandard_FK1] FOREIGN KEY (
[StandardID]
)
REFERENCES [dbo].[Standards] (
[StandardID]
)
GO

GO
```

Inject Example

TO: IT Staff
FROM: Pepper Pans
RE: Inject #4: Password Policy

We have discovered that our Active Directory password policy is unacceptably weak. Please fix this policy in Active Directory. This must be a NEW group policy with the name "Domain Policy." Do not append the new policy onto the existing Default Domain Policy. Place this new policy above all others in the list. Please keep the following requirements in mind when completing this task:

- Password History - Minimum of 16 re-uses
- Maximum Password Age - 42 days
- Minimum Password Age - 10 days
- Minimum Password Length - 10 characters
- Complexity Requirements - One of each of the following:
  - Uppercase Letter (A-Z)
  - Lowercase Letter (a-z)
  - Base 10 Digit (0-9)
  - Non-Alphanumeric Character such as: !@#$%^&*()+=

This request is to be completed by 12:30 PM today.

Domain

Access Control

Standard

CISSP

NIST

ISO

HIPAA

Control

NUMBER	NIST SP 800-53 CONTROLS	ISO/IEC 27001 (Annex A) CONTROLS

AC-1	Access Control Policy and Procedures	A5.1.1, A5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A10.1.1, A.10.8.1, A.11.1.1, A.11.2.1, A11.2.2, A11.4.1, A.11.7.1, A.11.7.2, A.15.1.1, A.15.2.1

Inject Scoring Example

Competition Event Scoring Instructions

Inject #1: Data Class & Labeling

Information Blue Team Received:

Our organization is contracted to do work for the federal government. As such, it is imperative that we maintain classification labels on all documents and emails produced so we can protect all levels of information appropriately. Please be sure to classify any documents or emails you produce as "Unclassified," "Sensitive but Unclassified," or "Classified." Do this through the use of headers and footers. Thank you.

This request should be adhered to for the duration of your employment with Shark Industries.

Time Due: Duration of Competition

Scoring Instructions (Remote):

Scoring this inject will involve collecting all document submissions (both email and tangible) and applying the following formula:

Number of Documents Submitted with Classification / Total Number of Documents Submitted = X

X * 5 = Total Points (round to two decimal places)