**Similarities:**

**Objective/Scope**: Although ISO 27002 is an international standard which works towards

the information security roles and responsibilities inside the organizations. PCI DSS works towards the customer card data and NIST CSF works towards prevention of cyber security threats and attacks, they all work towards handling the data with respective guidelines.

**Third Party assurance**: While most of the frameworks work with third parties and deal with the important data, the third party is selected through cautious due diligence and careful examination before engagement in the business.

**Risk Management**:ISO 27002, NIST CSF and PCI all have generated a wide range of standards, tests, matrices to validate and measure the security standards NIST SP 800-30 (Revision 1) totally focuses on the risk management in the organization. PCI DSS provides a roadmap for compliance to protect the cardholder data, and ISO 27002 does not define risk management standards as a control, but is amongst one of the three major security requirements described in information security measures.

**Access Controls:**When it comes to the access control, all the above frameworks and standards have a rigid rule. they all strive to make sure that only the right person should get the access to the network and data of the company, it should depend on the individual’s role. They give attention to auto-generated ID’s, passwords, authenticated access so that there are no loopholes for the hackers to misuse the data.

**Asset Management**: An asset can be referred to anything of value to the organization. IN PCI DSS context the assets refer to people, process and technologies, ISO 27002 refers asset to the entire network, while NIST CSF refers them to the maintenance to software and hardware the company uses, all the framework help categorizing the assets and their importance to the company.

**Information security policy**: All the frameworks thoroughly understand that to effectively enforce and audit security policies, the origination should first understand the system.ISO 27002, NIST CSF and PCI DSS, all three frameworks work towards achieving the confidentiality, integrity, secure data transmission, and configuration management of the data.

**Communication Security**: While most of the industries work with external vendors, communication is key factor be considered. PCI DSS makes sure that the cardholder data is encrypted while transmitted it over the network, to protect the data from security breaches. In NIST CSF (section 8, 9 and 12) all talk about the transmission integrity, confidentiality, and cryptography. ISO 27002(section 13.1 and 13.2) talk about the network security management and securing the information transfer.

**Dissimilarities**

**Scope**: While ISO 27002 is the only International standard published by an international organization of standards(ISO) and can be used by any organization, PCI DSS is very industry specific, meaning it is processed in the industry which deals with card holder data. Likewise, NIST is the National Institute of Standards and Technology address companies who mainly deal with cyber-attacks or threats, they can implement the NIST CSF framework.

**Acceptance**: ISO 27002 is accepted globally, NIST CSF is a united nation standards and is used widely in USA, PCI DSS is mainly used in Europe and north American region.

ISO 27002 is much friendlier to commercial business and can be referred and applied in any industry and do not require the involvement of security managers, while NSIT CSF mandates to have minimum security information as it classifies data, systems and detailed study of inventory where security data is stored. PCI CSS can be a part of any of the standards where cardholder data is processed.

**Flexibility**: ISO 27002 and NIST CSF are relatively flexible frameworks as compared to PCI DSS which requires the specified standards to be met. ISO 27002 can be disintegrated and does not require all the standards to be compliant.

**Auditing**: ISO 27002 is a multiyear cycle where a part is performed every year. While NIST and PCI DSS can be performed in one audit(yearly) and is followed by few network scanning audits.

NIST CSF is the only framework which carries out the evaluation of business environment and business supply chain, whereas ISO 27002 and PCI DSS won't.

**Business Continuity Plan**: PCI DSS is the only one who has widely implemented the Business Continuity Management i.e. disaster recovery for the cardholder data as compared to ISO 27002 and NIST CSF who depends on the incident management system which help set the procedures to follow the guidelines to recover and resume the services.