All the organizations today strive towards mainly one goal, the protection of the huge data they collect to run the business. Whether it is a bank, a retailer or an IT firm. They all adhere to some policies and procedures to follow the standards. Internal Audit is essential to check the professional success and failure transformations to help them grow. PCI DSS, ISO 27002 and NIST CSF are some of the frameworks the auditors use to evaluate the company. Even though they are used for the same purpose they have some similarities and few dissimilarities. The decision lies in selecting one over the other depending on the problem statement and the needs. Below points help us see the similarities and differences.

**Similarities:**

1.    **Objective/Scope**: Even though ISO 27002 is an international standard and PCI DSS and NIST CSF are just the frameworks and are used depending on the need of the business, they all work towards the same goal and are used for the same scope, that is to manage the information security of the company. The whole idea lies about making the security policies more rigid so that there is no scope for the invaders to misuse the data. All of them try and implement their best practices to secure the company from the malicious attacks.

**2.**    **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 particular attention to auto-generated ID’s, passwords, authenticated access so that there are no loopholes for the hackers to misuse the data.

3.    **Risk Management/Asset 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 defines risk management standards for the entire organization. An asset can be more or less 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.

4.    **Information security policy**: All the frameworks thoroughly understand that to effectively enforce the audit security policies, the origination should first understand the system.ISO 27002, NIST CSF and PCI DSS(section4.7) all three frameworks work towards achieving the confidentiality, integrity, secure data transmission, and configuration management of the data.

5.    **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**

**1.**     ISO 27002 is the only **International standard**published by an international organization of standards(ISO), NIST CSF is published by National Bureau of standards of USA and widely used in the USA. whereas the PIC DSS is just framework used where the card data is processed. The standards laid out in ISO 27002 acts as the benchmark of all other framework and most of the content is derived from ISO 27002.

2.    **Scope:**WhileISO 27002 is the only international standards, 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, while PCI DSS refers only to the cardholder industry.

3.    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.

4.    **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.

5.    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.

6.    **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.