**PCI-DSS**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

* Install and maintain a firewall configuration to protect cardholder data.
* Do not use vendor-supplied defaults for system passwords and other security parameters.
* Protect stored cardholder data
* Encrypt transmission of cardholder data across open, public networks
* Use and regularly update anti-virus software or programs
* Develop and maintain secure systems and applications
* Restrict access to cardholder data by business need to know
* Assign a unique ID to each person with computer access
* Restrict physical access to cardholder data
* Track and monitor all access to network resources and cardholder data
* Regularly test security systems and processes
* Maintain a policy that addresses information security for all personnel

**Conclusion:**

PCI-DSS provides a benchmark for the organizations to compare. It is a strong starting point and provides a strong base for feature security measures in an organization. But the main challenge in PCI-DSS is that we have to perform assessments to effectively analyze an organization. We need to use automation in compliance to save time and energy and efficiently monitor our system logs. We need to keep our system up to date and do periodic checks on the security of the system.

**ISO 27001/27002**

ISO 27002 is an internationally recognized standard designed for organizations to use as a reference for implementing and managing information security controls. The standard is intended to be used with ISO 27001, which provides guidance for establishing and maintaining information security management systems.

* Define, approve, and communicate a set of policies for information security.
* Review policies at planned intervals or if significant changes occur.
* Identify organizational assets and maintain an inventory of these assets.
* Classify information and assets in terms of value, criticality and sensitivity.
* Implement procedures to manage the use of removable media.
* Limit user access to the network and monitor use of network services.
* Restrict and control allocation and use of privileged access rights.
* Restrict access to information and applications based on access control policy.
* Password management systems should ensure quality passwords.
* Implement detection and prevention controls to protect against malware.
* Evaluate the organization’s exposure to vulnerabilities and address associated risks.
* Protect the transfer of information through all types of communication facilities.
* Review approach to managing information security at planned intervals.

<https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/iso-27002-compliance-guide.pdf>

**Conclusion:**

ISO 270001/270002 better organization with well-designed and managed processes and mechanisms. It promotes cost reduction with prevention of information security incidents. It also provides compliance with legislation and other regulations. One of the biggest shortcomings of ISO 270001/270002 is that the standard is too vague, it does not go into enough details. It also provides too much flexibility.

<https://advisera.com/27001academy/blog/2011/03/21/the-biggest-shortcomings-of-iso-27001/>

**CIS-Critical Security Control:**

The CIS Controls (formerly known as Critical Security Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

* Inventory and Control of Enterprise Assets
* Inventory and Control of Software Assets
* Data Protection
* Secure Configuration of Enterprise Assets and Software
* Account Management
* Access Control Management
* Continuous Vulnerability Management
* Audit Log Management
* Email Web Browser and Protections
* Data Recovery
* Incident Response Management
* Security Awareness and Skills Training

<https://www.cisecurity.org/controls/cis-controls-list>

**Conclusion:**