**Standards benefiting small and medium-sized businesses (SMEs).**

# Credentials

**Student Name: Syed Muhammad Haider Razvi**

**Student ID: M00832169**

**Module: Compliance & Project Management**

**Submission: 19th November 2023**

**CST2531**

**Compliance and Project Management** CST2531

Table of Contents

[Credentials 1](#_Toc151431602)

[1.0 - Introduction 3](#_Toc151431603)

[2.0 - Characteristics of SMEs 3](#_Toc151431604)

[**2.1 - Cybersecurity needs of SMEs** 4](#_Toc151431605)

[3.0 – Four international standards, their benefits & impact on textile oriented smes operating online 4](#_Toc151431606)

[**3.1 – ISO/IEC 27001: 2022** 5](#_Toc151431607)

[**3.2 – PCI DSS: PAYMENT card industry data security standard** 6](#_Toc151431608)

[**3.3 NIST Cybersecurity Framework (CSF)** 7](#_Toc151431609)

[**The five functions for CSF:** 7](#_Toc151431610)

[**3.4 ISO/IEC 20000-1:2018 (SERVICE MANAGEMENT SYSTEM FOR IT)** 8](#_Toc151431611)

[4.0 Gap Analysis of the selected standards 9](#_Toc151431612)

[5.0 – Conclusion 10](#_Toc151431613)

[Reference list 10](#_Toc151431614)

# 1.0 - Introduction

The word “International Organization” refers to standards designed by specialists associated with global organizations and coordinated by entities like ISO or the International Organization for Standardization. These standards ensure uniformity and quality in diverse industries (GenomSys, 2019).

International standards play a vital role in optimizing business operations, boosting productivity, and facilitating entry into new markets. International standards make it easier for businesses to enter diverse markets making it easier to export products and services internationally. International standards ensures that products and services meet recognized quality and safety benchmarks. This builds trust and confidence among consumers, which enhances the brand image. Technical standards promote collaboration and innovation among manufacturers, benefiting businesses as the products work smoothly together, which would enable local SMEs to be able to compete with the multi-national or large-scale companies and create a competitive environment in the market. Adhering to international standards eases market entry for businesses by gaining recognition from governments and regulatory bodies (CGBC, 2016).

Embracing international standards helps local SMEs meet global market needs, easing international exports. Standardized processes minimize costs by reducing errors, reducing waste, and increasing overall efficiency, by setting benchmarks, these standards encourage innovation and competitiveness, allowing SMEs to sustain a competitive advantage on a global scale. Minimizing costs will lead to enhanced annual Net Profit for local SMEs, annual Net profit for the local SMEs, allowing them to re-invest into the business. (SBS-SME, 2020).

Textile production holds significant importance for small and medium enterprises (SMEs) in Pakistan. The nation boasts a thriving textile industry, encompassing a diverse array of SMEs dedicated to the manufacturing of textiles, apparel, and various other textile goods.

# 2.0 - Characteristics of SMEs

Globally, SMEs are categorized based on factors like workforce size, assets, and annual turnover. However, in Pakistan, as outlined by the Ministry of Industries & Production and the National SME Policy Act (2021), Small Enterprises (SE) are businesses with valuations up to PKR 150 million and a staff not exceeding 50. Medium Enterprises (ME) span from above PKR 150 million to PKR 800 million, with employees ranging from 51 to 250 in manufacturing and services, and 51-100 in trading (Ministry of Industries & Production, Govt. of Pakistan, 2021).

Pakistan’s textile manufacturing sector plays a vital role in the nation's economy by producing fabrics, garments, and various textile goods. It confronts fierce global competition, necessitating adherence to international standards for market competitiveness, The sector has been consistently expanding, but it appears to have been significantly impacted by the economic downturn in recent years. Owing to rising economic challenges, the industry is presently operating below its full capacity (IFC, State Bank of Pakistan, 2011). Insufficient infrastructure exacerbates business costs, reducing profit margins (Punjab Economic Research Institute, 2020).

Diverse SMEs contribute to Pakistan's economy. Manufacturing SMEs produce textiles, garments, chemicals, and food. Service-based SMEs offer consulting, IT, healthcare, and education services. Retail SMEs engage in direct consumer sales through small shops and boutiques. Agriculture based SMEs focus on farming and food processing. Additionally, healthcare SMEs include small clinics, pharmacies, and healthcare service providers (Competition Commission of Pakistan, 2021).

## **2.1 - Cybersecurity needs of SMEs**

The significance of the Internet and computers for SMEs became evident after the COVID-19 crisis. To navigate the pandemic successfully, many small businesses adopted measures like incorporating cloud services, enhancing internet capabilities, upgrading websites, and facilitating remote work for their employees (European Union Agency for Cyber Security Needs, 2021). In today's world, with technology reaching its peak in SMEs especially after COVID-19, the risk of cyber-attacks is a notable concern.

However, to cater with Cyber-attacks, SMEs should take cybersecurity needs into consideration. Which could be, developing and regularly updating an Incident Response Plan for efficient handling and recovery. Implementing advanced network security, including firewalls and intrusion detection systems, strengthens defences against unauthorized access. Endpoint security, with antivirus and anti-malware solutions, minimizes the risk of unauthorized database access, reducing the likelihood of cyber-attacks for SMEs.

Bottom of Form

Other essential components encompass employee training, strict access controls, routine software updates. Solid backup plans boost resilience, ensuring swift responses to potential threats. Effective backup plans secure SMEs by reliably recovering critical data during cyber incidents, ensuring business continuity, minimizing downtime, and preserving customer trust. Regular security tests conducted by SMEs will guarantee the safety of their online websites containing personal and financial information, such as E-banking, credit cards, and emails (European Union Agency for Cyber Security Needs, 2021).

# 

# 3.0 – Four international standards, their benefits & impact on textile oriented smes operating online

ISO, or the International Organisation for Standardisation, is a non-governmental international organization that creates and publishes standards to assure quality, safety, and efficiency in different industries. An ISO standard is a globally accepted approach to performing a task, ensuring that everyone follows the same set of guidelines regardless of their location. This results in a more reliable and uniform outcome, benefiting both the organization and the end user. Companies can trust that the standard is consistently applied and recognized worldwide, providing them with a sense of assurance. Likewise, customers can be confident that the products or services they receive adhere to a standardized level of safety, quality, and reliability (Ideagen, 2023).

The International Electrotechnical Commission (IEC) is a worldwide body those issues standards for electronic and technical devices designed for consumer use. With participation from numerous nations, the IEC works towards establishing a uniform baseline standard for various types of electronic and technical products (Rouse, 2012).

## **3.1 – ISO/IEC 27001: 2022**

ISO/IEC 27001 is the most widely recognized standard for managing information security management systems (ISMS). It outlines the criteria that an ISMS needs to fulfil. The ISO/IEC 27001 standard provide direction to companies, regardless of size or sector, with instructions for creating, executing, sustaining, and consistently enhancing an information security management system. This ensures a comprehensive framework for safeguarding sensitive data, catering to companies across various industries and sizes. Compliance with ISO/IEC 27001 signifies that an entity has implemented a system to manage risks related to the security of its data. This system aligns with the best practices and principles outlined in the International Standard, reflecting the organization's dedication to ensuring secure data management (ISO, 2022). ISO 27001 is highly significant for textile enterprises involved in E-commerce and online transactions. It guarantees a strong information security management system, protecting vital data like customer information and transaction details. Adhering to this standard foster trust, creating a secure and dependable online space for both the business, its customer, and the suppliers

The textile small and medium enterprises (SMEs) operating through E-commerce handle sensitive information such as designs, customer data, and business strategies. ISO/IEC 27001 facilitates the establishment of controls and processes to ensure the confidentiality of this information. By implementing ISO/IEC 27001, these businesses demonstrate a dedicated commitment to information security, fostering enhanced customer trust and confidence. This is particularly crucial in the textile SME sector, where brand reputation plays a significant role in E-commerce success.

Moreover, as textile SMEs often rely on a network of suppliers and partners in their E-commerce operations, ISO/IEC 27001 proves valuable in managing and securing these relationships by establishing robust information security requirements for third parties. Considering the complexity of supply chains and business processes in the textile industry, effective risk management is vital for SMEs operating via E-commerce. ISO/IEC 27001 provides a systematic approach to identify, assess, and manage information security risks, thereby enhancing the resilience of these SMEs in the face of potential threats.

As these SMEs implement ISO/IEC 27001, they streamline processes and define roles and responsibilities related to information security, contributing to improved internal efficiency and effectiveness. This internal optimization is especially beneficial for textile SMEs in the E-commerce sector, where streamlined operations can positively impact competitiveness and customer satisfaction.

## **3.2 – PCI DSS: PAYMENT card industry data security standard**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards crafted to guarantee a secure environment for any business handling credit card information, the Payment Card Industry Data Security Standard (PCI DSS) aims to safeguard sensitive payment card data and reduce the risk of data breaches or cyber threats. The Payment Card Industry Security Standards Council (PCI SSC), a global organization formed by leading credit card companies such as Visa, MasterCard, American Express, Discover, and JCB, has established a set of requirements. The standard seeks to create a consistent and thorough structure for safeguarding payment card data and reduce or eliminate the credit/debit card frauds (RiskOptics, 2023).Bottom of Form

Placing PCI DSS will safeguard the customers’ important financial and personal data. An apparel or textile company places a high priority on establishing a strong firewall setup and using encryption algorithms for transmitted data when it comes to protecting consumer data. These safeguards are critical in protecting sensitive information like credit/debit card information and show the company's commitment to protecting customer privacy and establishing trust. Combating unauthorized access is also critical, which can be accomplished by avoiding default passwords and applying effective access control methods.

By doing so, the company not only decreases the risk of unauthorized access to its systems and consumer data, but also builds trust among its customers. Which can ultimately benefit the textile-oriented SMEs by making loyal customers, which can enhance the revenue and brand image. PCI DSS can help the textile SMEs operating via e-commerce as in the event of a data breach, the negative consequences on brand reputation and customer trust can be avoided by demonstrating of early security measure implementation. Utilizing up-to-date antivirus software and routinely testing security systems is crucial in safeguarding the business against emerging cyber threats. This practice minimizes the risk of data breaches and vulnerabilities in the system. Following these security practices ensures that the textile business complies with industry standards like PCI DSS. This alignment helps avoid penalties or legal problems related to data breaches. Following PCI DSS security practices can give the business a competitive advantage from its competitors. It signals to customers that the company values data security, potentially drawing in new customers and keeping the current ones satisfied (RiskOptics, 2023).

Although putting in place these security measures may require spending money initially, the potential financial consequences of a data breach or security incident can be much more significant. Investing in security measures from the start can lead to saving money in the long run by avoiding potential breaches and related problems.

## **3.3 NIST Cybersecurity Framework (CSF)**

The NIST Cybersecurity Framework is designed to aid businesses, regardless of their size, in gaining a clearer understanding of cybersecurity risks, effectively managing those risks, and minimizing them to protect their networks and data. It offers various businesses to set recommended practices to assist in prioritizing how to allocate time and resources for cybersecurity protection. (FederalTradeCommission, No Date).

The CSF streamlines cyber-risk management, enabling prompt and informed decision-making. Additionally, it simplifies the language of cybersecurity to enhance comprehension for both internal and external stakeholders. The CSF employs a straightforward framework consisting of only five primary functions, which are, Identify, Protect, Detect, Respond, and Recover (Cisco, 2023).

### **The five functions for CSF:**

**1- Identify**

The Identify feature assists in developing an overall risk management strategy for cybersecurity. It aids in the comprehension of your important assets, company environment, governance model, and supply chain (Cisco, 2023)

**2- Protect**

Protect assists in implementing crucial defensive measures by considering essential assets, and additional information provided by the Identify function. (Cisco, 2023).

**3- Detect**

Check the computers on a regular basis for unauthorized access or any unusual traffic from different software (Cisco, 2023).

**4- Respond**

The Respond function guides you in promptly undertaking appropriate measures through incident response planning, analysis, mitigation, communication, and continuous enhancement (Cisco, 2023)

**5- Recover**

The Recover function aids in restoring normalcy through recovery planning, ongoing enhancements, and effective communication (Cisco, 2023).

The online textile firm can systematically detect and mitigate cybersecurity risks by utilising CSF. CSF promotes a continuous improvement cycle, allowing online textile firms to adapt to changing cybersecurity threats and technology over time. Adopting CSF practices reflects a dedication to online security, showcasing a commitment to safeguarding sensitive customer information. In the context of the online textile industry, where customers share private details like credit/debit card information and customised designs, maintaining a reputation for security and trust is crucial for both attracting and retaining a customer base. Therefore, the implementation of CSF (Cyber Security Framework) is crucial for adoption in small or medium-sized textile businesses. It provides customers with the assurance that their personalized designs are securely safeguarded by the company. This not only eases customer worries but also removes the fears linked to possible cyber-attacks on the website of the company where they create their clothing designs. Due to its strong dedication to comprehensive cyber security measures, customers are inclined to have greater trust in the company.

## **3.4 ISO/IEC 20000-1:2018 (SERVICE MANAGEMENT SYSTEM FOR IT)**

This standard outlines the criteria for an entity to set up, execute, sustain, and consistently enhance a service management system (SMS). This standard outlines the things a company needs to do for planning, designing, transitioning, delivering, and improving services. The goal is to meet the needs of the services and bring value. This standard enables an organization to enhance the planning, design, transition, delivery, and improvement of services by efficiently implementing and operating an SMS. An organization can utilize this document to assess both its Service Management System (SMS) and the services it provides. This document is suitable for a customer looking for services and wanting assurance about the quality of those services (IS0, 2018).

This standard can be beneficial for the textile online business, as the services offered by textile small and medium-sized enterprises (SMEs) typically involve creating custom-designed clothing, providing style consultations, and production of garments. Additionally, textile businesses in apparel line may provide services related to alterations or modifications to ensure that the clothing fits the customer's preferences and requirements. Overall, the work of SMEs in textile sector involves providing a range of creative and personalized services to meet the unique needs and preferences of their clients.

ISO/IEC 20000-1 offers a structure for creating, and consistently enhancing a service management system, ultimately resulting in heightened service quality and increased customer satisfaction for the online textile or apparel business. Aligning with ISO/IEC 20000 showcases the dedication to delivering high-quality services, which boosts customer confidence and trust in the online textile business. This has the capacity to give customer satisfaction, maintain loyalty, and repeat business. The standard highlights the importance of having efficient service delivery processes. The adoption of ISO/IEC 20000-1 can streamline the business operations, leading to a reduction in errors and delays during service delivery. Thus, this will enable textile SMEs to create positive relationships with their suppliers.  
Timely and error-free delivery is crucial in a textile business providing services for both custom-made and ready-made garments. Delays in expected deliveries can erode customer confidence. Through process optimization and pinpointing areas for enhancement, the implementation of ISO/IEC 20000-1 has the potential to enhance the efficiency of the business, ultimately resulting in long-term cost savings. Which can enhance the annual turnover and Net profit for the business.

# 4.0 Gap Analysis of the selected standards

The selected ISO standards, namely ISO/IEC 27001:2022, PCI DSS, NIST Cybersecurity Framework (CSF), and ISO/IEC 20000-1:2018, collectively address crucial aspects of information security, data protection, and service management. For local SMEs, particularly in the textile sector operating via E-commerce, adherence to these standards yields positive effects. ISO/IEC 27001 ensures robust information security management, fostering customer trust and compliance with regulatory requirements. PCI DSS safeguards financial and personal data, enhancing brand reputation and customer loyalty. The NIST CSF offers a comprehensive framework for cyber-risk management, contributing to a resilient defence against evolving threats. ISO/IEC 20000-1 streamlines service management, optimizing processes for customized clothing and alterations, leading to improved efficiency and customer satisfaction.

However, challenges may arise for local SMEs, including initial financial investments in compliance and ongoing maintenance costs. While these standards strengthen local businesses, there might be concerns regarding the accessibility and affordability of compliance for smaller enterprises.

In the context of worldwide commerce and cooperative efforts, following established standards bring about overall advantages. These standards play a vital role in creating a shared foundation for crucial aspects such as information security, data protection, and service quality. Consistent adoption of these standards builds trust among international partners, thereby promoting collaboration and facilitating trade. Nevertheless, there is a potential drawback if strict compliance becomes a hurdle for smaller businesses aiming to engage in the global marketplace. This highlights the importance of implementing and supporting these standards in a balanced manner to ensure inclusivity and foster global cooperation.

# 5.0 – Conclusion

In conclusion, the adoption of international standards such as ISO/IEC 27001, PCI DSS, NIST Cybersecurity Framework (CSF), and ISO/IEC 20000-1 by local small and medium-sized enterprises (SMEs) in Pakistan's textile sector, operating via E-commerce, offers substantial benefits in terms of information security, data protection, and service management. These standards provide a robust framework for building trust, enhancing customer satisfaction, and ensuring compliance with regulatory requirements. While challenges, including initial financial investments and ongoing maintenance costs, may arise, the long-term advantages, such as improved efficiency, customer loyalty, and resilience against cyber threats, outweigh these concerns.

However, challenges such as initial financial investments and ongoing compliance costs may pose concerns for local SMEs. Despite these challenges, the consistent adoption of international standards establishes a shared foundation, building trust among global partners and facilitating international trade. It's important to find a middle ground between enforcing strict rules and being flexible enough to support smaller businesses. This balance is essential for encouraging collaboration on a global level. Ultimately, the implementation of cybersecurity measures and commitment to international standards not only protect SMEs but also enhance their competitiveness, expansion, and enduring prosperity in the ever-changing digital environment.

# Reference list

‘What is an International Standard?’. (2019) GenomSys, Available at: <https://genomsys.com/internation-standard-and-its-benefits/> (Accessed: 16th November 2023).

‘Benefits of International Business’. (2016) CGBC, Available at: <https://www.cgbusinessconsulting.com/benefits-international-standards/> (Accessed at: 16th November 2023).

‘Why should SMEs care about standards?’. (2020) Small Business Standards, Page 3. Available at: <https://www.sbs-sme.eu/sites/default/files/A%20Practical%20Guide%20for%20SMEs_EN.pdf> (Accessed: 16th November 2023).

‘Small and Medium Enterprises Development Authority: SME Policy 2021’. (2021) Government of Pakistan, Ministry of Industries & Production, Page 9. Available at: <https://moip.gov.pk/SiteImage/Misc/files/SME%20Policy%202021.pdf> (Accessed: 16th November 2023).

‘Features of SMEs’. (No date) Know it all Ninja, Available at: <https://www.knowitallninja.com/lessons/features-of-smes/> (Accessed: 16th November 2023).

'ANALYSIS OF TEXTILE AND CLOTHING SECTOR TRADE: INNOVATIVE PRACTICES AND THE WAY FORWARD'. (2020) Government of the Punjab, Publication NO. 460. Available at: <https://peri.punjab.gov.pk/system/files/Textile%20report%20design%20%281%29.pdf> (Accessed: 16th November 2023).

‘IFC Advisory Service in the Middle East and North Africa’. (2011) State Bank of Pakistan, Page-4. Available at: <https://www.sbp.org.pk/departments/ihfd/Sub-Segment%20Booklets/Textile%20Fabric.pdf> (Accessed: 16th November 2023).

'Enhancing the Economic Efficiency of Small and Medium Enterprises in Pakistan'. (2023) Competition Commission of Pakistan, Available at: <https://cc.gov.pk/assets/images/Downloads/assessment_studies/enhancing_the_economic_efficiency_of_smes_in_pakistan.pdf> (Accessed: 16th November 2023).

‘Cybersecurity guide for SMEs, 12 steps to securing your business’. (2021) European Union Agency for Cyber Security Needs, Page 2-10. Available at: <file:///Users/haiderrazvi/Downloads/ENISA%20Cybersecurity%20guide%20for%20SMEs-online-single_page.pdf> (Accessed: 16th November 2023).

‘What are ISO standards?’. (2023) Ideagen, Available at: <https://www.ideagen.com/thought-leadership/blog/what-are-iso-standards#:~:text=An%20ISO%20standard%20is%20essentially,the%20customer%20or%20end%20user>. (Accessed: 16th November 2023).

Margaret Rouse. (2012) ‘International Electrotechnical Commission’, Techopedia, Available at: <https://www.techopedia.com/definition/7673/international-electrotechnical-commission-iec> (Accessed: 16th November 2023).

‘ISO/IEC 27001:2022’. (2022) ISO, Available at: <https://www.iso.org/standard/27001> (Accessed: 16th November 2023).

'ISO 10007:2017'. (2023) ISO, Available at: <https://www.iso.org/standard/70400.html> (Accessed: 16th November 2023).

‘Cloud Computing’. (2023) bsi, Available at: <https://www.bsigroup.com/en-GB/Security-controls-for-cloud-services-ISO-IEC27017/Benefits-for-cloud-service-customers/> (Accessed: 16th November 2023).

'What Are PCI DSS Standards?'. (2023) RiskOptics, Available at: <https://reciprocity.com/resources/pci-dss-standards/> (Accessed: 18th November 2023).

'Understanding the NIST Cybersecurity framework' (No date) Federal Trade Commission, available at: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework> (Accessed: 18th November 2023).

'What Is the NIST Cybersecurity Framework?'. (2023) Cisco, Available at: <https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html> (Accessed: 18th November 2023).

'ISO/IEC 20000-1:2018'. (2018) ISO, Available at: <https://www.iso.org/standard/70636.html>  
 (Accessed: 18th November 2023).

'ISO/IEC 20000-1:2018'. (2018) PMG, Available at: <https://www.pmgame.net/iso-iec-20000-1-2018.php> (Accessed: 18th November 2023).