

# MICROSOFT WINDOWS ASSESSMENT AND SECURITY

## PENDRIVE (MS WAASP)



By

Abdul Rehman Janjua

A thesis submitted to the faculty of Information Security Department,  
Military College of Signals, National University of Sciences and Technology,  
Islamabad, Pakistan, in partial fulfillment of the requirements for the degree of MS in  
Information Security

September 2021



## THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Abdul Rehman Janjua Registration No. 00000203806, of Military College of Signals has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have been also incorporated in the said thesis.

Signature: \_\_\_\_\_

Supervisor: Assoc Prof. Dr. Haider Abbas

Date: \_\_\_\_\_

Signature (HoD): \_\_\_\_\_

Date: \_\_\_\_\_

Signature (Dean): \_\_\_\_\_

Date: \_\_\_\_\_

## ABSTRACT

With technological advancement, our community is getting more linked day by day than we have ever been previously. However, while such advances make our everyday life convenient, they also increase additional exposure to our data. Hence, making it difficult for individuals and corporations to flourish in an extraordinarily complicated and challenging landscape. Mainly, issues such as adopting appropriate enterprise administration practices to tackle data breaches and monetary scandals, the variety of corporate exposure, and legal requirements exert influence on corporate administration to develop a comprehensive solution or utilize the existing solution. However, the current approaches for identifying and managing risk are either unreliable or too complicated and overpriced for usage by every company or single person. As a result, we employed a structured method to suggest a cost-effective and dependable solution. In order to develop a comprehensive solution, this thesis lays down a foundation in order to be compliant with Information Security Standards in the context of Operating System, as a result safeguarding the information resources.

Moreover, it concentrates on the windows platform retrieving the data critical for making the Operating System compliant with Information Security Standards like NIST SP 800-53. Finally, it lays out the framework for securing the Windows system, which users can adopt, and calculates the percentage compliance of the assessed PC. To make the process of compliance easy, a proof-of-concept solution (toolkit) is constructed for automatically auditing the Windows operating system's security and consistently validating the gap within the standard and current configurations on Windows machines. To validate the framework, the toolkit was used to scan a windows PC. The toolkit examines windows machines' compliance state by producing a comprehensive report for the system. Finally, an operating system security strategy has been presented; companies or individual users may implement that to assure compliance with NIST SP 800-53.

**Keywords** — Security Standard Compliance, Operating System Hardening, Cyber Security Standard, Security Auditing, Automation

# DEDICATION

*This thesis is dedicated to*

*MY FAMILY AND TEACHERS*

*for their love, endless support and encouragement*

## **ACKNOWLEDGEMENTS**

I am grateful to Allah, the Almighty, for His mercy and benevolence who has bestowed me with the strength and the passion to complete this thesis. Without his consent I could not have indulged myself in this task.

I am also thankful to my supervisor especially and committee members who have always guided me with their keen and useful counseling in achieving my research objectives.

# TABLE OF CONTENTS

<b>THESIS ACCEPTANCE CERTIFICATE</b>	<b>iii</b>
<b>ABSTRACT</b>	<b>iv</b>
<b>DEDICATION</b>	<b>v</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vi</b>
<b>LIST OF FIGURES</b>	<b>x</b>
<b>LIST OF TABLES</b>	<b>xi</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 The primary causes of software security vulnerabilities . . . . .	1
1.3 Issues on End of Users . . . . .	2
1.4 How can digital assets be protected? . . . . .	2
1.5 The general worldwide market of various Operating Systems . . . . .	3
1.6 Problem Statement . . . . .	4
1.7 Major Contributions of Research . . . . .	5
1.8 The Research's Scope . . . . .	6
1.9 Organization of the thesis . . . . .	6
<b>2 SECURITY STANDARDS AND APPLICATIONS</b>	<b>8</b>
2.1 Introduction . . . . .	8
2.2 Security and Hardening . . . . .	8
2.3 Cybersecurity Standards . . . . .	9
2.4 Applications of Cybersecurity . . . . .	10
2.4.1 Healthcare . . . . .	10
2.4.2 Finance . . . . .	10
2.4.3 Retail . . . . .	11
2.4.4 Energy . . . . .	12
2.4.5 Defense . . . . .	13
2.4.6 Consumer Information . . . . .	13

<b>3</b>	<b>CYBERSECURITY ATTACKS AND VULNERABILITIES</b>	<b>15</b>
3.1	Cybersecurity attack statistics . . . . .	15
3.2	Vulnerabilities Identified in Microsoft (MS) Windows . . . . .	15
3.3	Windows 95 . . . . .	17
3.4	Windows 98 . . . . .	17
3.5	Windows 98 Second Edition (SE) . . . . .	18
3.6	Windows Millennium Edition (ME) . . . . .	18
3.7	Windows XP . . . . .	18
3.8	Windows Vista . . . . .	19
3.9	Windows 7 . . . . .	20
3.10	Windows 8 . . . . .	20
3.11	Windows 8.1 . . . . .	21
3.12	Windows 10 . . . . .	21
3.13	Industry-Wide Cybersecurity Practices . . . . .	22
3.14	Selection of Security Standards . . . . .	24
<b>4</b>	<b>LITERATURE REVIEW</b>	<b>26</b>
4.1	Related Research Work . . . . .	26
4.2	Existing Security Standards . . . . .	32
4.2.1	National Institute of Standards and Technology (NIST) . . . . .	32
4.2.2	Federal Information Processing Standards (FIPS) . . . . .	34
4.2.3	ISO/IEC 27001-2 . . . . .	34
4.2.4	Common Criteria (CC) . . . . .	34
4.3	Existing Software Tools . . . . .	36
4.3.1	Acuity STREAM . . . . .	36
4.3.2	Vigilant Software(vs) Risk . . . . .	36
4.3.3	Microsoft Baseline Security Analyzer (MBSA) . . . . .	37
4.3.4	Microsoft Security Assessment Tool (MSAT) . . . . .	37
4.3.5	Belarc Advisor . . . . .	37
4.3.6	Lynis . . . . .	38
4.3.7	Open Security Content Automation Protocol (OpenSCAP) . . . . .	38
4.3.8	Tiger . . . . .	38
4.3.9	Center for Internet Security (CIS) Configuration Assessment Tool . . . . .	39
<b>5</b>	<b>CYBERSECURITY FRAMEWORKS</b>	<b>41</b>
5.1	NIST Cybersecurity Framework (CSF) . . . . .	41
5.1.1	Core . . . . .	41
5.1.2	Implementation Tier . . . . .	42



5.1.3	Framework Profile . . . . .	43
5.2	CC Cybersecurity Framework . . . . .	43
5.2.1	Target of Evaluation . . . . .	44
5.2.2	Protection Profile (PP) . . . . .	44
5.2.3	Security Target . . . . .	44
5.2.4	Security Functional Requirements . . . . .	44
5.2.5	Security Assurance Requirement . . . . .	45
5.2.6	Evaluation Assurance Level . . . . .	45
5.3	ISO Cybersecurity Framework . . . . .	45
5.3.1	Scope . . . . .	46
5.3.2	Normative References . . . . .	47
5.3.3	Terms & Definitions . . . . .	47
5.3.4	Context of the Organization . . . . .	47
5.3.5	Leadership . . . . .	47
5.3.6	Planning . . . . .	47
5.3.7	Support . . . . .	48
5.3.8	Operation . . . . .	48
5.3.9	Performance Evaluation . . . . .	48
5.3.10	Improvements . . . . .	48
5.4	FIPS Cybersecurity Framework . . . . .	48
5.4.1	Level 1 . . . . .	48
5.4.2	Level 2 . . . . .	49
5.4.3	Level 3 . . . . .	49
5.4.4	Level 4 . . . . .	50
<b>6</b>	<b>PROPOSED FRAMEWORK FOR WINDOWS</b>	<b>51</b>
6.1	Proposed Framework Steps . . . . .	51
6.1.1	Security Controls . . . . .	51
6.1.2	Security Controls Categorization . . . . .	52
6.1.3	Evaluate System . . . . .	53
6.1.4	Check Compliance . . . . .	53
<b>7</b>	<b>VALIDATION OF PROPOSED FRAMEWORK</b>	<b>56</b>
<b>8</b>	<b>FUTURE WORK AND CONCLUSION</b>	<b>58</b>
8.1	Conclusion . . . . .	58
8.2	Future Work . . . . .	58
	<b>BIBLIOGRAPHY</b>	<b>58</b>

# LIST OF FIGURES

1.1	Desktop market share of Various Operating Systems . . . . .	4
1.2	Market Share of Windows versions in Pakistan . . . . .	5
2.1	Applications of Cybersecurity . . . . .	11
3.1	Windows Malware Attacks Source Data . . . . .	17
3.2	Windows Distribution of Malwares in 2017 . . . . .	17
3.3	Windows Distribution of Malwares in Quarter-1 of 2018 . . . . .	18
3.4	Vulnerabilities in Windows 95 . . . . .	19
3.5	Vulnerabilities in Windows 98 . . . . .	19
3.6	Vulnerabilities in Windows 98SE . . . . .	20
3.7	Vulnerabilities in Windows ME . . . . .	20
3.8	Vulnerabilities in Windows XP . . . . .	21
3.9	Vulnerabilities in Windows Vista . . . . .	21
3.10	Vulnerabilities in Windows 7 . . . . .	22
3.11	Vulnerabilities in Windows 8 . . . . .	22
3.12	Vulnerabilities in Windows 8.1 . . . . .	23
3.13	Vulnerabilities in Windows 10 . . . . .	23
5.1	NIST Cybersecurity Framework . . . . .	44
5.2	CC Cybersecurity Framework . . . . .	45
5.3	ISO-IEC Cybersecurity Framework . . . . .	46
6.1	Proposed Framework . . . . .	55
7.1	Internet Explorer and Firefox vulnerable to Poodle Attack . . . . .	56
7.2	Unsigned Software . . . . .	57
7.3	Unencrypted Drives . . . . .	57
7.4	Event Logs Access Rights . . . . .	57
7.5	Autorun Settings . . . . .	57

# LIST OF TABLES

2.1	Organizations which Defined Cybersecurity Standards . . . . .	8
3.1	Cybersecurity Standards Usage Statistics . . . . .	25
4.1	Related Research Work . . . . .	28
4.2	Security Compliance Standards and Supported Controls . . . . .	35
4.3	Existing Software Tools with Supported Security Standards and OS . . . . .	39
5.1	Categories of Proposed Set of Requirements . . . . .	49
6.1	Security Controls . . . . .	52
6.2	Security Controls Categorization . . . . .	52

## **INTRODUCTION**

### **1.1 Overview**

Small to Large companies have been striving hard to secure and safeguard their digital assets against unauthorized access from being exploited and abused by malicious individuals. These evil individuals may range from disgruntled insider employees to keen entities with a barrage of resources to infiltrate information systems using the Internet. With the ever-increasing attacks landscape, the Cybersecurity field is becoming part and parcel of modern information technology [1]. Modern computing devices are no longer restricted to large bulky workstations but instead comprise of various devices such as smart television, laptops, cellphones, etc. These little computing devices are backed by microcontrollers which are actively being utilized in the Internet of Things. As with any technological field, there is a need for standardization from a security point of view. To achieve this purpose, many Cybersecurity standards have been formalized for different domains and are enforced by the companies to safeguard their digital assets.

As the amount and complexity of Cyber-attacks are growing tremendously [2], according to US intelligence officials, cyber-attacks and digital spies are becoming the top threat, even overshadowing terrorism [3]. Some infamous Cyber-attacks examples include Yahoo 2013 (3,000,000,000 records) [4], First American Corporation 2019 (885,000,000) [5], Facebook 2019 (540,000,000) [6]. Furthermore, ransomware such as Locky [7], WannaCry [8], Bad Rabbit [9], and Petya [10] have cost millions of dollars in losses in recent years, affecting every industry throughout the world. The main reason for such attacks is security flaws in the design or the implementation of the software used by the businesses. Both software applications and operating systems can introduce security bugs, but the Operating system is the nucleus of any computing device; if security flaws are introduced in the Operating System configurations, it introduces myriad security flaws throughout the system.

### **1.2 The primary causes of software security vulnerabilities**

As we have established, software design flaws are a dominant contributor to privacy and security breaches in enterprise applications and operating systems [14], with a substantial chunk originating from developers creating insecure code. Even though various techniques and methods [15] were

investigated by the cybersecurity enthusiasts and software development industries to promote secure software development, the magnitude of the matter has not been considerably reduced. Some of the reasons why the software developers have been unable to follow these security practices are discussed below:

One of the primary reasons is technological competition between different software development companies as they try to release new versions of software to market in a relatively short period. One such example is the release of a new Android Operating System version every few months. These releases sometimes vary from minor updates to full-fledged revamped major versions [16]. The competitor of Android OS, Apple IOS, also follows similar time-frames with minor differences and releases major and minor upgrades of the Operating System [17]. These unrealistic timelines for the launching of newer versions put a great deal of pressure on software engineers. To rub salt to the wounds of these software engineers, the software developers need to design the updated revision of software that must be more efficient and competent than the prior one. Thus, innovative features that will attract consumers must be designed and programmed. Mostly in case of minor revisions, more functionalities are added, and previous bugs are fixed. Due to the enhancement of functionality, the software's design and architecture are altered, which needlessly complicates software development, making the whole process complex and tedious. The last but significant technical difficulty the software engineers face is the tight schedules, leaving little to no time for programmers to verify and test the program before delivering it to the consumer. As previously stated, the entire situation becomes the primary basis of a massive number of flaws inside the program [18],[19]. Once a newer version of the software is launched to the consumer, cybersecurity experts and hackers attempt to identify the flaws, and a list of shortcomings is rapidly [20], [21].

### **1.3 Issues on End of Users**

System administrators and end-users who do not have proper training and knowledge about Cybersecurity are frequently ignorant of the minor aspects of best practices and system configurations, which may jeopardize the system's security. Despite if they are educated, it is standard practice to prioritize usability over security. Therefore, organizations cannot identify any irregularities in the security configurations and entirely fail to protect their computer from intruders.

### **1.4 How can digital assets be protected?**

To safeguard against cyberattacks and other security issues, numerous cybersecurity standards have been developed to oversee the use of cybersecurity technology in various sectors. However, some

of these standards only provide the industry's best practices, recommendations, and guidelines for safeguarding the information represented on computing devices. To accept these best practices as standards, teams from reputed academia and security professionals from different organizations collaborate to put forward the security standards. Over time organizations have developed sets of laws and guidelines that have acquired global recognition as standards. Some of these standards focus on specific devices, while some of these standards are generalized and applied to most computing devices. One of the most well-known security standards is Common Criteria (CC), which provides 13 different device categories [11]. Unfortunately, these regulations are presented concisely, leaving plenty of room for interpretation [12]. Another well-known standard known as NIST SP 800-53 offers controls and guidance to maintain the confidentiality, integrity, and availability of digital assets and data, officially known as the CIA triad [13].

These security standards are often applied to data at rest, in motion, and in use. Fine-grained features include password security, firewalls, anti-malware, anti-virus, encryption, decryption, system user training, and system administrator preparedness, among other things. Some of these standards may have resulted from legislation governing how data is accessed, managed, and handled. For system security assessment and vulnerability scanning, particular toolkits are developed by OS manufacturers and private entities. However, identifying security problems, misconfiguration, and flaws is nearly complicated for a typical user. Likewise, even for a company with expertise in Cybersecurity, the challenge of becoming compliant with a specific standard is time-consuming. Microsoft has developed a security compliance manager [22], which can alter and maintain system parameters via a well-organized user interface. However, cybersecurity guidelines are broad and do not address specific operating systems (OS) issues. As a result, hardening a machine, even with Microsoft Security Compliance Manager, becomes a time-consuming job for an end-user since the user must manually collect all OS-related criteria from multiple standards.

## **1.5 The general worldwide market of various Operating Systems**

The present-day operating systems are built to support many users, multitask, and handle many distinct tasks at once. According to data collected by StatCounter [23], Microsoft Windows operating systems are by far the most prevalent and widely used desktop operating systems, capturing 73.54% of the market share. The OSX ranks as the second widely used operating system with 15.87%. In contrast, Linux comes at 4 th place and has a market share of about 2.38%, as shown in Figure 1.1. As we have identified, Microsoft Windows is the most widely used Operating System globally, so

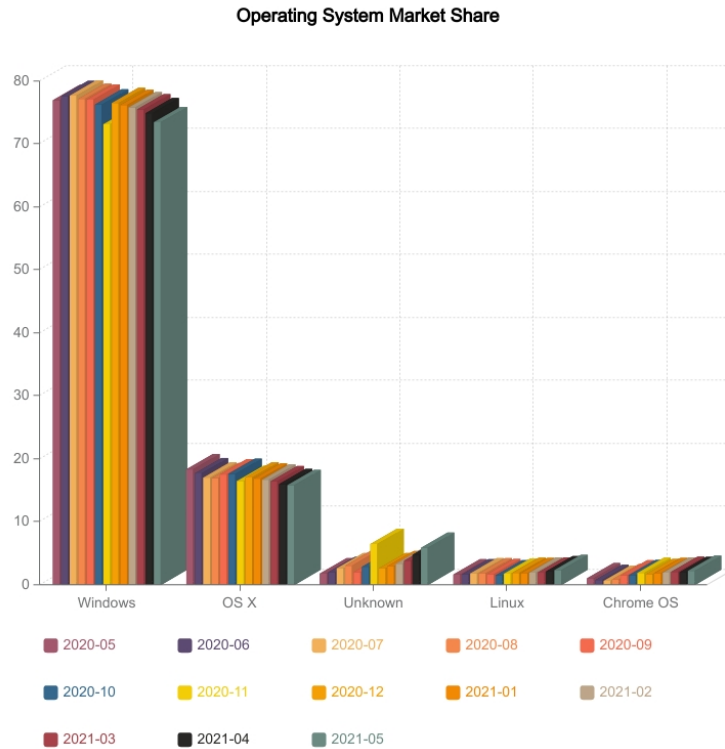


Figure 1.1: Desktop market share of Various Operating Systems (May 2020 till May 2021)

we decided to explore further the various versions of the Windows Operating system and its market share in Pakistan. StatCounter [24] shows that Windows 10 captures a 63.26% share of the market, whereas the 2 nd most used version of Windows is Windows 7 with 28.74%, which can be seen in Figure 1.2. Because of the increased popularity of Windows 10 due to its attractive user interface and built-in security modules and Microsoft ending the support of Windows 7, the market share of Windows 10 is increasing [25]. We developed a technique for assessing security configurations of the Windows 10 operating system of end-users, which is used by both end- users and businesses.

## 1.6 Problem Statement

There is currently no comprehensive Cybersecurity framework or standard that provides in-depth security for hardening and securing the Operating System. Most of the Cybersecurity frameworks are fragmented, which are unable to adequately capture complete corporate security requirements in context to operating systems. Hence, a extensive framework is needed [27], [28], [29]. To develop more efficient Cybersecurity, frameworks for specific tasks, mostly universal frameworks, particularly NIST and ISO/IEC 27001, are utilized. However, ideal cyber defense is challenging to attain without a clear knowledge of what complete Cybersecurity defense is and how it could be achieved[30]. Typically, business companies ignore cost, operational considerations, and attackers'

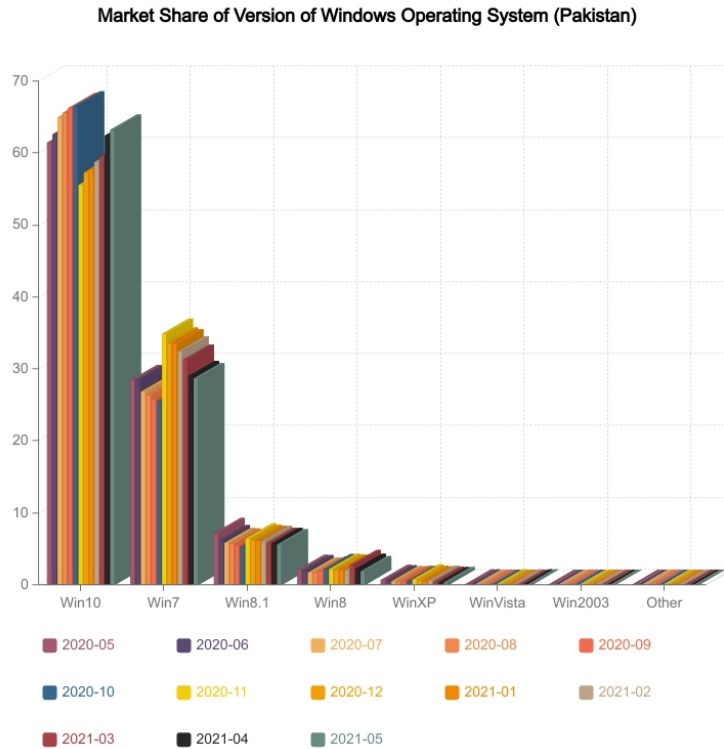


Figure 1.2: Market Share of Windows versions in Pakistan (May 2020 till May 2021)

capabilities even if they have some internal framework to help them harden their operating system. Another issue that most companies face is that the operating system securing and hardening is solely dependent on the skills of the support engineers and sometimes feedback of the pen-testing teams.

In order to protect from external threats and develop a coherent security configuration of the Operating System, a toolkit has been developed that would enable the end-user to scan their operating system's security configuration and discover security gaps between the framework and the operating system. The suggested solution simplifies adding new computing devices in an organization by implementing the same framework and can help identify the security gap between the newly installed device and the security framework. It will help the average user by masking the complexity of the framework from them. It would lower the training expenses for both end-users and system administrators.

## 1.7 Major Contributions of Research

This thesis provides an in-depth study, extensive analysis, and comparison of current cybersecurity standards. Finally, we propose a list of basic minimum requirements for OS hardening based on our research.



This thesis makes the following significant contributions:

1. A thorough examination of current cybersecurity standards.
2. In-depth study of the NIST, FIPS, CC, and ISO 27001/2 frameworks.
3. A comparison of the aforementioned cybersecurity requirements in relation to operating systems.
4. A summary of the vulnerabilities and exploits found in various versions of Microsoft Windows, ranging from Windows 95 to Windows 10.
5. Classification of diverse industries impacted by cyber risks, based on the adoption of cybersecurity policies.
6. A comprehensive study of the most frequently used software solutions to ensure compliance with cybersecurity requirements.
7. Proposed a framework for operating system hardening.
8. A toolkit that scans the system to identify the security gap between the framework and the current Operating System configurations.

## **1.8 The Research's Scope**

The research applies to Windows 10, but it may also be used to evaluate security compliance for Windows versions following Windows 7, which are being actively used for residential and business purposes. The toolkit will help the end-users to strengthen their security infrastructure by adhering to globally recognized standards.

## **1.9 Organization of the thesis**

Chapter 1 introduces the research topic and presents the problem statement. After identification of the problem, it highlights the need for a solution for the research problem. Furthermore, the solution to the identified problem is presented. Chapter 2 discusses security and various security standards and their application areas. Chapter 3 summarises historical data on cybersecurity attacks and vulnerabilities discovered in Microsoft Windows due to non-compliance with cybersecurity standards.

Additionally, this part discusses the reasoning behind the cybersecurity criteria used for this study. Chapter 4 summarises the classification of the literature, including relevant studies, data on essential

security standards, and software solutions. Chapter 5 provides an in-depth examination of cyber-security frameworks. Chapter 6 presents the security framework for Windows 10, which is further implemented in a toolkit. Chapter 7 tests the proposed framework by using the toolkit. Chapter 8 summarizes the study and makes some recommendations for further research.

## SECURITY STANDARDS AND APPLICATIONS

### 2.1 Introduction

Before digging into the depths of Cybersecurity, it is critical to get a basic understanding of the subject, its standards, and applications. This chapter provides an overview of the various cybersecurity disciplines.

### 2.2 Security and Hardening

OS hardening is the practice of improving the security of an operating system and its network architecture to maintain and increase its effectiveness. The security of an operating system may be enhanced by adopting correct settings, removing vulnerable services, upgrading software, and enforcing security rules, such as raising password strength and analyzing user logins. The level of hardening is determined by corporate policies and the network administrator's abilities [31]. The most frequent method is to adhere to preset security procedures that are run periodically to guarantee compliance with security standards. Auditing technologies, such as the Open Security Content Automation Protocol, can be used to execute pre-configured lists (OpenSCAP). Hardening controls comprise various administrative control procedures, a collection of rules that comply with applicable government requirements, and corporate security standards. These considerations need the use of automatic hardening scripts (e.g., OpenSCAP), generalized hardening tools (e.g., Microsoft Baseline Security Analyzer), access control tools (e.g., Tiger, Security-Enhanced Linux (SELinux)), and the deployment of network restrictions (e.g., firewalls).

Table 2.1: Organizations which Defined Cybersecurity Standards

Sr.	Organizations	Standard
1.	International Organization of Standardization (ISO) [32]	ISO/IEC 27001-2

2.	National Institute of Standards and Technology (NIST) [33]	NIST SP 800-53
3.	Center of Internet Security (CIS) [34]	CIS Controls
4.	Information System Audit and Control Association (ISACA) [35], [36]	The Risk IT Framework
5.	Information Security Forum (ISF) [37]	ISF's Standard for IS
6.	International Telecommunication Union (ITU) [38], [39]	ITU GCA
7.	The European Telecommunications Standards Institute (ETSI) []	ETSI-Security Standards
8.	Data Interchange Standards Association (DISA) [20],[21]	DISA-Cyber Security Standard
9.	Information Technology Infrastructure Library (ITIL) [22], [23]	ITIL-Security Management
10.	IEEE (Institute of Electrical and Electronic Engineers) [24], [25]	C37.240-2014
11.	The Payment Card Industry Security Standards Council (PCI SSC) [26]	PCI Security Standards
12.	The Internet Engineering Task Force (IETF) [27], [28]	IETF-Internet Standards
13.	Open Web Application Security Project (OWASP) [29]	OWASP-ASVS
14.	International Legal Technology Association (ILTA) [30]	ILTA Peer-Security Practices
15.	Common Criteria (CC) [31], [32]	CC-Cyber Security
16.	Organization for the Advancement of Structured Information Standards (OASIS) [33], [34]	OASIS Standards

### 2.3 Cybersecurity Standards

Predefined security standards from NIST, CC, and ISO, among others, can be applied for system maintenance and improvement. Manually securing and verifying each machine on the network is a

time-consuming process. Network administrators can actively adhere to these security requirements to strengthen the OS's security. An autonomous system may exist to evaluate the system's overall integrity and provide a summary based on current configurations. Numerous reputable groups have issued cybersecurity guidelines. Table 2.1 contains a list of these organizations.

## **2.4 Applications of Cybersecurity**

The last decade has seen considerable growth in the number of guidelines and regulations governing Cybersecurity across all industries. Several significant sectors include healthcare, finance, defense, energy, retail, and consumer data, as seen in Figure 2.1. The following section provides an in-depth examination of how cybersecurity rules are being implemented in these six key areas.

### **2.4.1 Healthcare**

Cyber attackers see the healthcare industry as a valuable target. Though financial institutions face the most significant risk of cyberattack, the health system has been one of the most targeted sectors since 2015. Numerous cybersecurity applications are built on the Internet of Things (IoT), which connects cyberspace to the real world. Healthcare IoT apps capture patient data via Electronic Health Records from a variety of sources (EHR). This information can be sent or kept in the cloud [35], [36]. The Health Insurance Portability and Accountability Act sets the bar for cybersecurity compliance in the healthcare business (HIPAA). It develops standards for all entities involved in the healthcare business, whether directly or indirectly. Healthcare apps handle extremely sensitive and personal user data. As a result, it is difficult to protect such critical data from different kinds of threats that might result in the exposure and security breach of crucial data [37], [38], [39].

### **2.4.2 Finance**

State and federal regulators have proposed many cybersecurity rules and regulations for the banking industry. The Federal Financial Institutions Examination Council (FFIEC) establishes the majority of the industry's standards that can be found in its manual [40]. This guidebook is divided into many volumes detailing the regulations and resources that financial institutions must adhere to. Likewise, several other principles are shared by different legal organizations. Additionally, the Financial Industry Regulatory Authority (FINRA) establishes many rules and regulations that the financial services sector must follow. It demands the submission of documented processes and policies for the protection of customer-sensitive information against cyberattacks. Additionally, these rules detail techniques for identifying and mitigating cyber- threats [38], [38], [38] Improve the consumer's identity [38], [38], [38]. Significant advancements in the distribution of web-based material enable a



Figure 2.1: Applications of Cybersecurity

revolution in the field of information systems.

Additionally, cloud-based technologies enable the creation of exceptionally diverse models for digital assets. These quickly developing patterns have wreaked havoc on the industry's standards from a cybersecurity standpoint. Likewise, the cybersecurity insurance business is a growing segment of the financial services sector, providing a specialized set of coverage and reactive assistance to firms that experience data breaches, among other things. Nonetheless, many cybersecurity risks must be addressed and standardized [41], [42].

### 2.4.3 Retail

The retail industry is primarily attacked for the credit card data it keeps for end-users, among several other businesses. Merchants must adhere to the Payment Card Industry Data Security Standard to solve this risk (PCI DSS). A federal agency does not govern this industry; instead, it adheres to PCI DSS rules, which require businesses that handle payment-related data to comply to reduce fraudulent efforts or the danger of security breaches [43]. PCI DSS establishes standards for the transmission and storage of payment-related information in order to reduce the risk of fraud or data breach. To

ensure operational security and compliance, merchants must use various security measures to assure compliance with specific regulatory standards and, lastly, generate compliance reports to verify standard compliance. This standard protects cardholders' sensitive data from well-known credit card issuers, including MasterCard Worldwide, Visa Incorporated, American Express, JCB International, and Discover Financial Services. According to PCI DSS requirements, one of the major concerns is data security. As a result, every provider organization that interacts with the processing of credit card info must adhere to the PCI DSS criteria [44]. PCI DSS uses industry-standard security methods to safeguard cardholder data, and its deployment can be regarded as a prudent move. This standard contains high-level (twelve) specifications that must be adhered to and details the information security best practices different retailers and credit card issuers must implement. The PCI's safety and the result are contingent upon the frameworks used. PCI compliance's real essence depends upon completing three steps: assess, remediate, and report. While a robust cybersecurity standard focuses on protecting information assets decided by people and supported by well-documented processes, such as guidelines, procedures, and policies, some companies focus on process, technology, and current operations improvement. However, their primary concentration on the areas mentioned above leads to obliviousness to the human (people) component of information technology [45].

#### **2.4.4 Energy**

Advances in the energy sector's digitalization have resulted in enormous economic advantages, most notably through simplifying and enhancing the efficiency of the energy consumption process. However, such developments in this industry have raised the possibility of cyber-attacks. Recent cyber-attacks on Ukraine's power generation have emphasized the rising relevance of this ever-present danger. As a result, during the last several years, the US and EU have consistently pursued compliance with various laws and policies to defend the energy industry from possible cyber-attacks. There are significant distinctions between the EU and US methods [46]. The US favored an approach of in-depth security with comprehensive and stringent regulations in specific areas. Still, the EU established an extensive and flexible structure addressing a broad range of concerns while avoiding substantial precise maneuvers relevant to member states' application of standards.

The US plan is far more advanced than the EU framework regarding cybersecurity regulations and their implementation. Nevertheless, at the distribution system, the US may seek assistance from their EU counterparts in particular areas, such as Cybersecurity for data protection, privacy, and network security. The goal is to promote regulatory alignment between the US and the EU to establish uniform cybersecurity standards. In this situation, the existence of significant distinctions between the

United States and the European Union may create several problems. Cybersecurity exemplifies a considerable possibility to strengthen transatlantic partnership in the following years [47, 48].

#### **2.4.5 Defense**

The defense sector's nexus has shifted dramatically during the last two decades. Extortion from classic insurgent operations is no longer the military sector's primary concern. Nowadays, advancements in the information technology area, such as reconnaissance systems, sophisticated weaponry with surveillance and intelligence capabilities, and a massive volume of sensitive data, need the use of upgraded and trustworthy cybersecurity solutions. The current cybersecurity industry offers diverse solutions, including application security, data, cloud security, wireless and network security, and end-point security. These solutions can perform various functions and could be integrated to create robust protection against multiple threats using a multi-layered strategy.

Cyber-attacks' intricacy ranges from viruses to sophisticated tactics such as zero-day attacks, Stealth Bots, Dynamic Trojan Horse Network worms, which compel cybersecurity firms to develop sophisticated protection solutions. These technologies include information security management (SIM), network traffic analysis, integrating a basic unified threat management system, next-generation firewalls, distributed denial of service (DDoS) protection, safelist, and security information and event management (SIEM). The growing threat of cyber-attacks on vital organizations from various organized criminal groups, along with specific technological advancements in the cybersecurity industry, continues to be a significant driver of the growth of cybersecurity solutions. Homeland and defense agencies are expected to account for roughly 40% of the global cybersecurity industry in 2015 [49]. Allocation of money for different military initiatives, including research & innovation of cybersecurity solutions for combat ground communication systems, is expected to continue as the most significant future direction in the cybersecurity business for the defense industry.

#### **2.4.6 Consumer Information**

Each year, cyber-attacks result in the theft of vast amounts of data and the appearance of tarnished reputations. Customers are increasingly concerned than ever about privacy and security concerns posed by increasingly sophisticated cyber-attacks. Regardless of the business, Cybersecurity has attracted significant attention in recent years as hackers attempt to steal critical data and intellectual property, and financial and personal information. The digitalization of data substantially influences various businesses, but technological developments have negatively affected the consumer industry. Due to stricter privacy regulations and the development of innovative gadgets like Alexa, Siri, and Google Home, the consumer data collecting business is on the verge of imploding. Companies and



organizations with direct access to customer data, such as consumer goods manufacturers, retailers, and restaurants, must take the necessary steps to avoid and minimize cyber risks throughout the digitization process.

Since consumer data is frequently associated with transaction channels for procurement, security for consumer-related businesses has taken on a more considerable relevance to safeguard Personally Identifiable Information (PII) from identity theft. As noted before, security standards for operating systems and other application fields of Cybersecurity are a need and an essential element of every industry that interacts directly or indirectly with computer systems, the Internet, and technology. Due to the unique dangers to public safety and the potential for considerable financial loss, organizations should examine the universal security measures outlined in a range of linked legislation and industry standards. Whichever risk management security control or strategy is implemented inside the company, the critical point is to utilize an integrated and automated security architecture capable of operating significantly and quickly.

Additionally, the explosion in the number of different systems, platforms, and linked devices demonstrates that vulnerability and manual asset management are insufficient. Organizations are being compelled to develop interactive and interconnected security measures to stay up with evolving risk factors. As a result, they must verify their compliance with a variety of legal and industrial standards. They should bear in mind that compliance alone may not be a successful security strategy. Alternatively, the new laws and standards require companies to pay proper attention when implementing controls and solutions to detect and manage risks [50], [42].

## **CYBERSECURITY ATTACKS AND VULNERABILITIES**

This section highlights many recent high-profile cybersecurity incidents, followed by the reasons why businesses struggle to comply with various security requirements. Following that, data on malware attacks and Microsoft vulnerabilities are given to emphasize the need to adhere to information security standards. Lastly, the present state of compliance with the relevant standards is discussed.

### **3.1 Cybersecurity attack statistics**

As we move into this digital age, the dreaded issue of Cybersecurity is perpetually raised. The World Economic Forum [51] ranks global-scale cyber-attacks as one of the world's top five serious risks.

These cyberattacks endanger ordinary citizens and multinational organizations as the information disclosed by such cyberattacks are critical. Marriott Hotels, British Airways [52], MyFitnessPal [53], TicketFly [54], and My-Heritage [55] are just a few of the international organizations that have had security breaches in 2018.

According to some estimates [56], the threat landscape is expanding rapidly, that the impact of cybersecurity losses will exceed \$6 trillion by 2021. As a result, it is not an overstatement to say that Cybersecurity is a critical problem for today's businesses and organizations. One of the primary causes for these attacks is that few firms take industrial standards and regulations seriously. According to the survey [57], just 23% of businesses adhere to industry standards. Some of the cases cited in the report were the following:

1. Like the Network and Information Security Directive, mandatory cybersecurity law is prioritized, even though it is costly to implement and takes most funds and effort.
2. There is a shortage of competent personnel with expertise in compliance with cybersecurity standards.
3. Security standards evolve rapidly and are sometimes hard to follow: compliance with 2018 requirements doesn't automatically comply with 2019 standards.

### **3.2 Vulnerabilities Identified in Microsoft (MS) Windows**

Considering Microsoft Windows has been the most widely used operating system in terms of users, malware developers attack it more commonly than other operating systems. Between 1995 and 2003,

numerous vulnerabilities in Windows 95, Windows 98, and Windows XP were reported [58]. From 2008 to 2015, attacks on Windows computers increased steadily as cyber thieves recognized the enormous potential in this area. However, attacks began to drop around 2016 but appear to be reviving around 2017 [59], as illustrated in Figure 3.1. Figure 3.2 depicts the spread of Windows-based malware during the year 2017. Likewise, Figure 3.3 shows the propagation of Windows-based malware in the first quadrant of 2018. The data of these pie charts were created using information taken from the AV-Test report (P-6) [60]. A summary of various malware variants for Windows OS demonstrates the types of attacks that cybercriminals found advantageous in 2017, shown in Figure 3.2. Cybercriminals have devoted their time, resources, and effort to determine which form of malware was most profitable for spreading their mission.

Trojan horses accounted for over 40% of malware targeting Windows. They became the best malware option for cybercriminals in 2017 due to their ability to destroy the target computer upon successful infection. They are frequently loaded with additional malicious functionalities, making them a malware equivalent of a Swiss army knife. Following Trojans are viruses, which account for about 26% of the market; meanwhile, JavaScript-based malware accounts for approximately 18.5 percent of the market. Typically, these scripts operate in the background and communicate with the c&c server. Password Trojans account for around 4.50 percent of the market; they usually capture login credentials and confidential credit card details. Worms, which often propagate via networks and whose primary objective is self-replication, accounted for 4.29 percent of the market. Backdoors, which enable malware developers to infiltrate and access a victim's system without the victim's knowledge, account for around 1.39 percent of the market share. Dialers, which allows cyber criminals to call premium service lines in return for financial rewards, account for less than 0.01% of the market. Exploits represent less than 0.08 percent of all vulnerabilities in Windows, and the knowledge necessary to build a Windows exploit is extremely rare as Microsoft releases patches to fix these exploits. Bots comprise around 0.20 percent of malware. Hackers primarily administer these bots, which allows them to carry out targeted attacks such as Distributed Denial of Service (DDOS) attacks. Apart from these malware types, there are a few more that account for almost 0.08 percent and execute a variety of illegal functions. Since 1995, Microsoft has released a number of operating systems. Several prominent Windows operating systems are covered individually below, alongside their vulnerabilities. Additionally, the security vulnerabilities discovered each year for the operating system are listed in Figures 3.4-3.13.

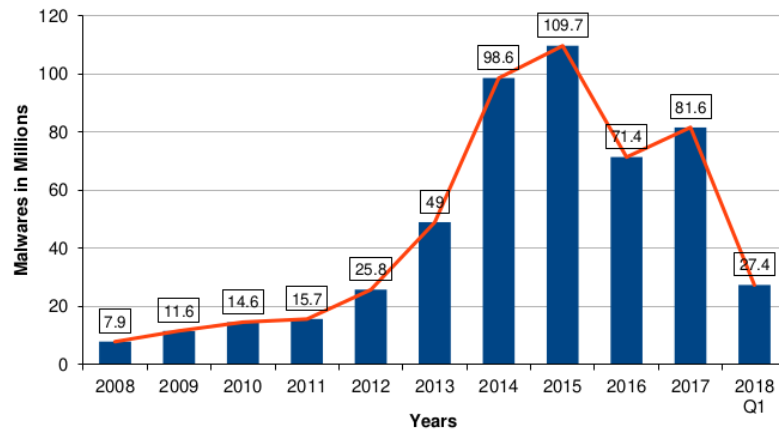


Figure 3.1: Windows Malware Attacks Source Data

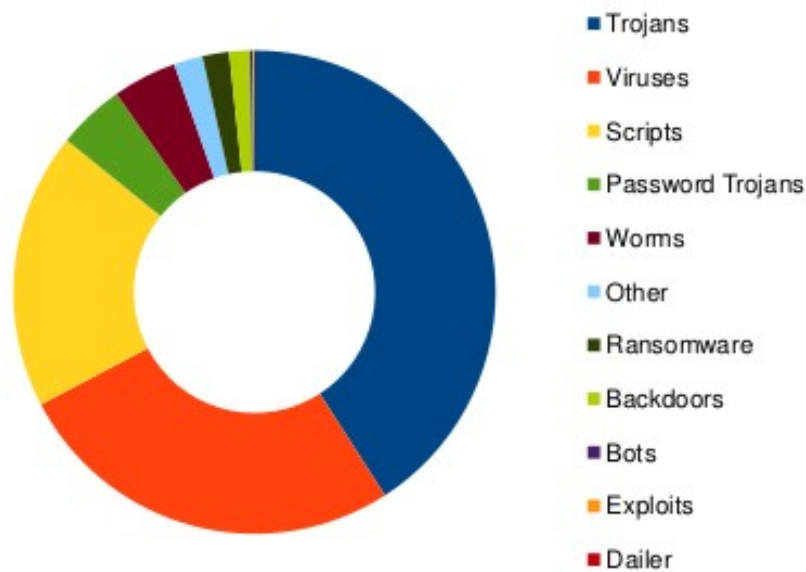


Figure 3.2: Windows Distribution of Malwares in 2017

### 3.3 Windows 95

On August 24, 1995, Microsoft released Windows 95. It was made using fairly basic MS DOS’s architecture. It did, though, directly handle 32-bit programs, as well as plug and play compatibility for new devices and a range of additional capabilities. However, the transition from DOS to Windows mode resulted in the discovery of several vulnerabilities that were exploited. Figure 3.4 summarises the approximately 36 vulnerabilities found to date [61], which include denial of service, code execution, buffer overflow, security-check bypass, and privilege escalation.

### 3.4 Windows 98

On June 25, 1998, Microsoft released Windows 98. It was a successor to the preceding Windows 95 version, introducing the Windows driver model, supporting new technology like USB-based pe-

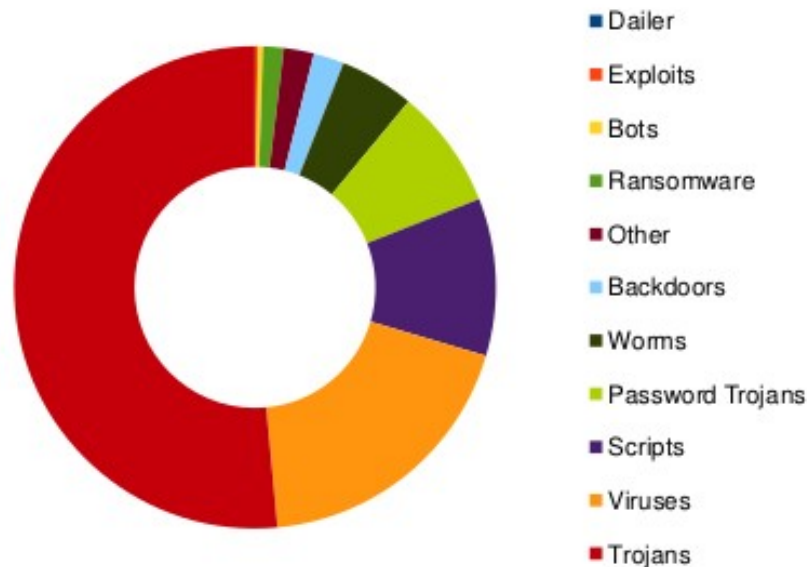


Figure 3.3: Windows Distribution of Malwares in Quarter-1 of 2018

ipherals and other essential features. With the release of Windows 98, the number of vulnerabilities increased. About 84 vulnerabilities have already been identified, including denial of service attacks, code execution, buffer overflows, and privilege escalation via system bypass. Figure 3.5 summarises the number of vulnerabilities discovered each year for Windows 98.

### 3.5 Windows 98 Second Edition (SE)

MS Windows 98 SE was released in May 1999 and included improvements such as Internet Explorer 5.0 and Windows Media Player 6.2. It addressed several problems discovered in Windows 98, reducing the overall number of security flaws to about 61, as seen in Figure 3.6.

### 3.6 Windows Millennium Edition (ME)

MS Windows ME was released around starting of the millennium (September 14, 2000). As with its predecessors, Windows ME was built on the Windows 9x architecture; however, access to MS-DOS was restricted to speed up the operating system's startup time. Fifty-eight vulnerabilities have been already discovered to date, including denial of service attacks, code execution, buffer overflows, memory manipulation, Cross-Site Scripting (XSS), and privilege escalation via system bypass, as seen in Figure 3.7.

### 3.7 Windows XP

MS Windows XP was released on October 25, 2001, marking a significant shift from its predecessors as it moved away from the MS-DOS-based paradigm favoring Windows New Technology

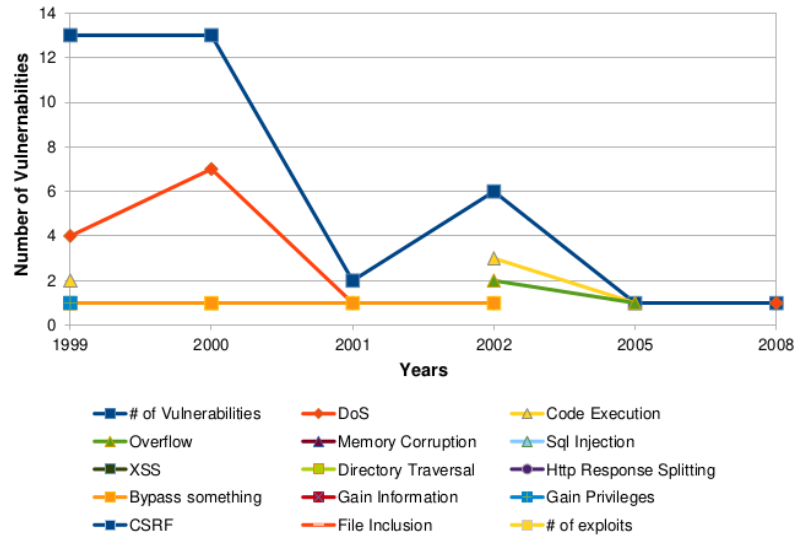


Figure 3.4: Vulnerabilities in Windows 95

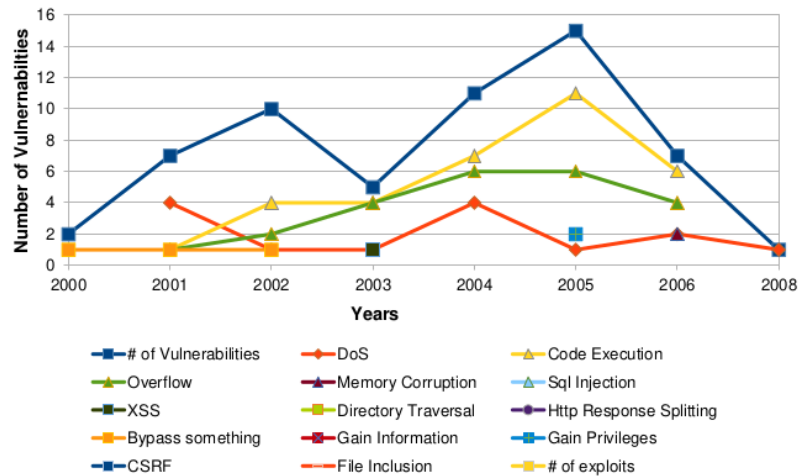


Figure 3.5: Vulnerabilities in Windows 98

system. It enhanced networking capabilities, simplified multimedia, and offered Remote Assistance. As depicted in Figure 3.8, Windows XP contains around 740 documented vulnerabilities, including escalating rights by surpassing system protection, memory corruption, Cross-Site Scripting (XSS), and escalating privileges by overcoming system security.

### 3.8 Windows Vista

On November 30, 2006, Microsoft released Windows Vista, which included innovative features such as a redesigned user interface and increased security. As seen in Figure 3.9, eight hundred twenty-eight vulnerabilities have been identified in Windows Vista.

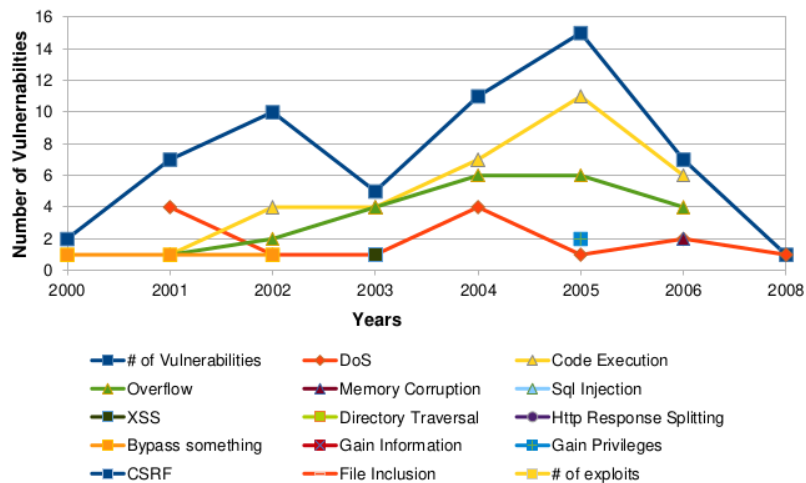


Figure 3.6: Vulnerabilities in Windows 98SE

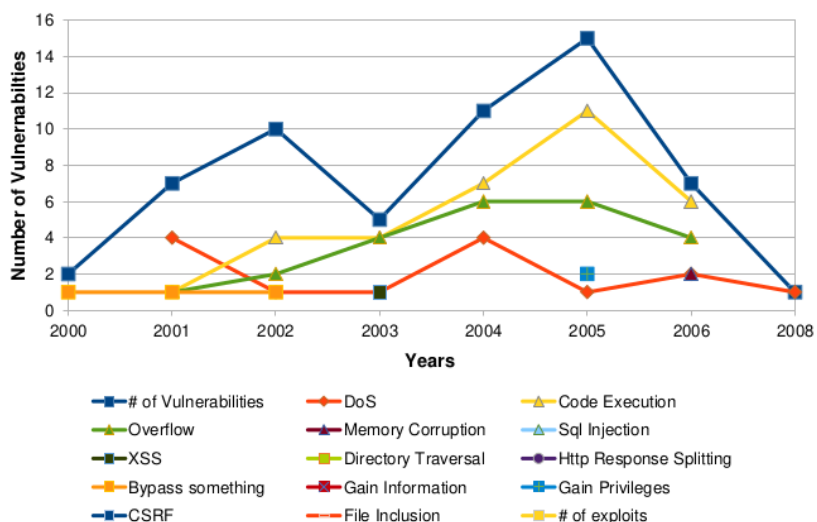


Figure 3.7: Vulnerabilities in Windows ME

### 3.9 Windows 7

MS Windows 7 was released on July 22, 2009, and included new features, like multi-touch capabilities, built-in networking, and other enhancements. One thousand one hundred and three vulnerabilities in Windows have already been identified thus far, as seen in Figure 3.10.

### 3.10 Windows 8

On October 26, 2012, Microsoft released Windows 8, which included advanced functionality such as multi-touch capability, home networking capabilities, and other enhancements. Windows 8 introduced a change to the user interface, which was accomplished via Microsoft Metro Design's usage and an emphasis on touchscreen devices. As seen in Figure 3.11, two hundred and fifty-six vulnerabilities have been identified in Windows 8.

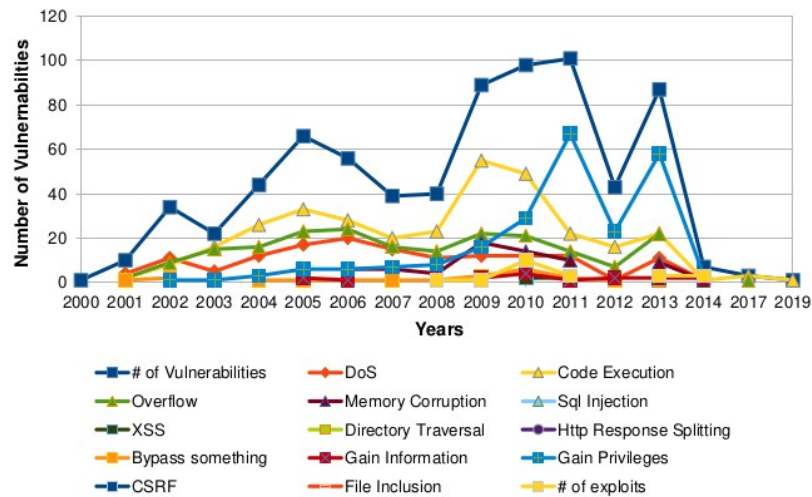


Figure 3.8: Vulnerabilities in Windows XP

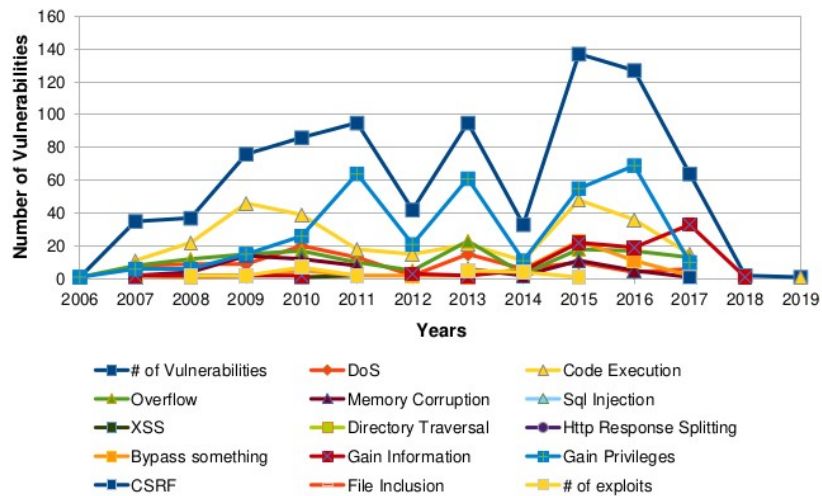


Figure 3.9: Vulnerabilities in Windows Vista

### 3.11 Windows 8.1

MS Windows 8.1 was released on October 17, 2013, and included new features like customizable live tile sizes and an in-depth connection with Microsoft OneDrive. Eight hundred fourteen vulnerabilities in Windows 8.1 have been disclosed, as described in Figure 3.12.

### 3.12 Windows 10

On July 29, 2015, Microsoft released Windows 10. It reintroduced the menu bar, virtual desktop, amongst other functionalities. Since the launch of Windows 10, a total of 851 vulnerabilities have been identified, as seen in Figure 3.13.



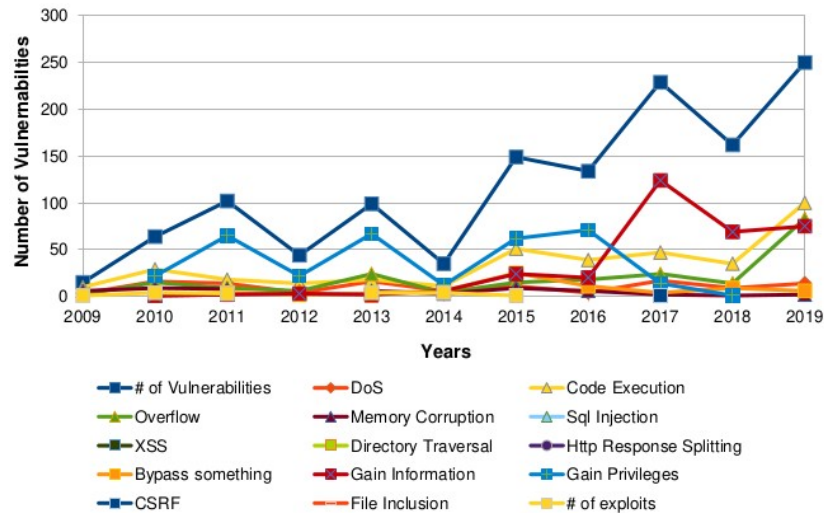


Figure 3.10: Vulnerabilities in Windows 7

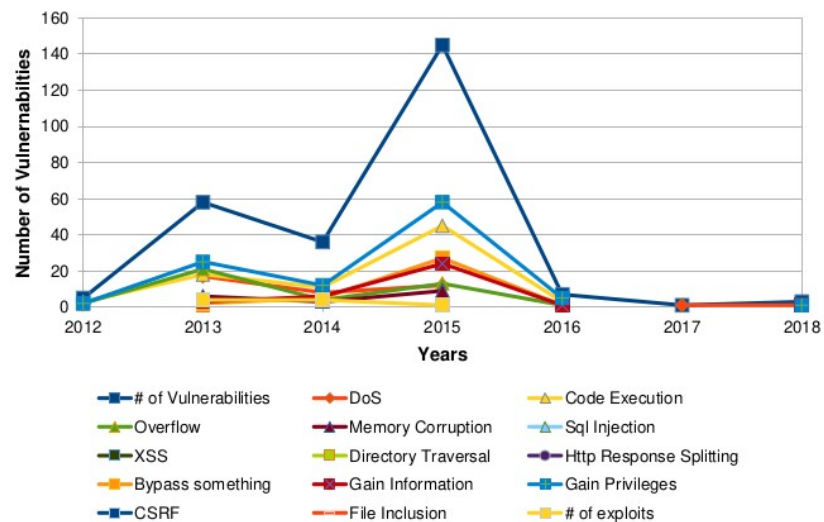


Figure 3.11: Vulnerabilities in Windows 8

### 3.13 Industry-Wide Cybersecurity Practices

In theory, every business, government, and other body should follow industrial and professional best practices to secure information technology (IT) assets, customer data, and additional information. Unfortunately, there is still a gap between perception and reality, which are sometimes exceptionally far. According to relevant studies, the majority of businesses lack adequate data security procedures and do not adhere to industry and professional standards. This creates weaknesses that can result in the loss of data, cash, and credibility. The following are some of the most salient aspects of contemporary cybersecurity scenarios:

- ZDNet [62] reported that security accounts for less than 2% of IT spending.
- According to The SSL Store [63], over 70% of the workforce in the United States are unaware

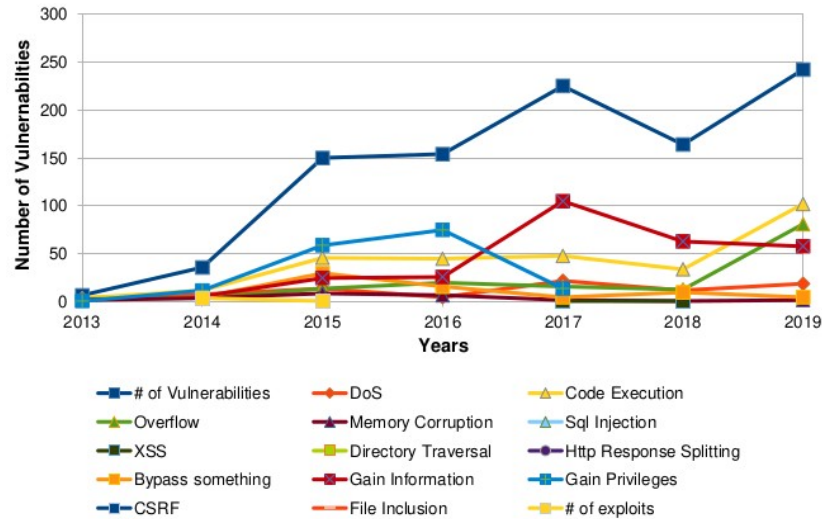


Figure 3.12: Vulnerabilities in Windows 8.1

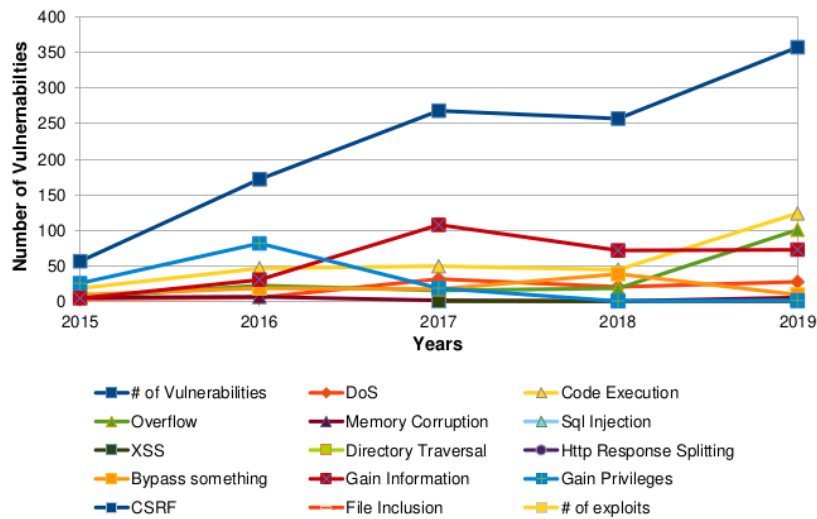


Figure 3.13: Vulnerabilities in Windows 10

of cybersecurity.

- According to High-Tech Bridge [64], 32% of the US and 16% of European nations failed to deploy TLS/SSL certificates.
- Verizon [65] reports that about 52.5% of businesses were utterly compliant with PCI/DSS standards in 2017.
- According to Why No Https [66], approximately 30% of the leading 560 webpages are not secure.
- According to a survey released by Tech Republic [67], approximately 93% of businesses have password policies, just under 25% have enforced password changes compulsory, and 53%

demand quarterly updates.

- As per Bullet Proof's [68] yearly report, 22% of hypercritical incidents are caused by missing security patches and the use of out-of-date software.
- According to Cisco research [69], 68% of US businesses do not choose to go for cybersecurity assurance.
- As per NationWide [70], 68% of businesses lack a disaster recovery plan (DRP). Additionally, it has been claimed that 71% of smaller companies never purchase business interruption insurance.
- According to Nciper [71], approximately 45 percent of businesses have a standardized encryption policy. Only About 50% of these companies revealed that they are using encryption throughout the entire organization.
- According to BDO USA [72], 73% of companies comply with bare-minimum cybersecurity standards.
- According to Global Market Insights [73], the security size is forecast to reach \$300 billion by 2024, up from the original \$1.5 trillion [74].

These figures demonstrate the severe importance of overcoming the cybersecurity barrier in all areas.

### **3.14 Selection of Security Standards**

Several cybersecurity standards have been addressed in the previous section, and these standards are extensively implemented in a wide variety of businesses. Nonetheless, according to a survey conducted in 2018 by HIMSS Cybersecurity Survey, the most widely used standard is specified by the National Institute of Standards and Technology (NIST), which is used by over 58% of participants. The NIST framework was created to address the cybersecurity concerns of important enterprises by providing administrative advice for risk management. These regulations are based on industry best practices and guidelines, allowing further enhancement by establishing additional standards. Around 26.4% of firms adhere to the Health Information Trust Alliance (HITRUST) framework, which is an association of healthcare corporations that addresses health care security problems. HITRUST is followed by Critical Security Controls CIS, which has a market share of nearly 24.7%.

The Center for Internet Security (CIS) is a non-profit organization that oversees the SANS 20 Critical Security Controls designed to withstand common attacks. Around 18.5% of respondents indicated

that they adhere to ISO security requirements. ISO is a not-for-profit organization dedicated to publishing international standards and best practices to facilitate global trade. The ISO has about 160 member nations. Around 7.3% of respondents stated that they adhere to the Control Objectives for Information and Related Technologies (COBIT) framework issued by the Information Systems Audit and Control Association [75]. Table 3.1 contains this information.

Table 3.1: Cybersecurity Standards Usage Statistics

Sr.	Standard	Percentage
1.	NIST	57.9%
2.	HITRUST	26.4%
3.	Critical Security Controls	24.7%
4.	ISO	18.5%
5.	COBIT	7.3%
6.	Other	5.1%
7.	No security framework	16.9%
8.	Don't know	8.4%

## LITERATURE REVIEW

This chapter reviews previous research on compliance with specific security requirements and describes in detail the different security standards that apply to operating systems. Additionally, current software applications and technologies have been explored, as well as their shortcomings.

### 4.1 Related Research Work

Teodoro et al. [76] presented a general model for using critical organizational variables such as human resources, technology, and processes. Additionally, it displays the compliance rate with NIST's cyber-security framework. Their methodology quantifies current cybersecurity risks, assigns monetary values to stated compliance goals, and eliminates resource overlap. The primary objective is to advise businesses and to direct cybersecurity techniques in accordance with cybersecurity frameworks.

Giulio et al. [77] examined the four commonly deployed information technology security standards, assessed their effectiveness for handling current cloud security threats, and highlighted weaknesses left unresolved in these frameworks. The authors proposed critical changes to address essential requirements of security in light of the current threat landscape. It focuses on general information technology security by thoroughly examining standards and making suggestions and recommendations.

Duncan, Bob Whittington, and Mark [78] recommended using typical checklist techniques to ensure certain security criteria are adhered to. They do not, though, provide the guarantee of provision of security assurance. The complexity of IT relationships and the rigidity of compliance, audit, and other processes might mismatch security goals. While it conducts a thorough study and evaluation of standards regarding their growth, recognized enhancements, and faults that need to be addressed, it concentrates only on generic information technology security. They provide suggestions but do not propose a solution.

Piromsopa et al. [79] presented a cyber insurance scoring methodology based on the outcomes of internal and external audits and compliance with mandatory and voluntary requirements. The scoring approach is based on adherence to applicable standards, including PCI DSS, HIPAA, SOX, Basel, and ISO 27001. Their model is mainly geared toward insurance firms for internal and external audits.

Pardo et al. [80] proposed a taxonomy for integrating disparate reference models and defining the critical concepts that may be used to consolidate them. Additionally, researchers stated that UML establishes a basis for depicting information in an orderly manner by illustrating relationships across entities/models. Users may easily read and comprehend UML diagrams since they do not need any knowledge. Additionally, they offer a structured method for generating related ideas and similarities among various models. A web-based solution is given that has been used to unify several models, including COBIT [81], Basel II, RISK IT, VAL IT, ITIL, and ISO 27002.

Pardo, César, Pino, and coworkers [82] conducted a survey in which researchers identified many unification strategies for various model types, including Align, Mapping, Combine, and Merge. Additionally, they found numerous research studies that have unified (a) two reference models, (b) more than two reference models, and (c) two or more reference and assessment models. Their paper emphasizes the significant differences in the components, terminology, and methods that obstruct the unification of diverse models.

Mellado et al. [83] established the Security Requirements Engineering Process, which is built on several Common Criteria (CC) components (SREP). SREP analyses security needs using CC structures, such as the protection profile, security management components, and different security assurance components.

Li et al. [84] collected responses from IT experts regarding the security aspect of virtualization using a questionnaire survey on the ISO/IEC27001 standard's 133 controls. Additionally, they used the Content Validity Ratio to determine which controls to select based on the study. Evaluations were conducted using the data gathered via these surveys.

Alsaleh et al. [85] proposed a security analytics architecture that increases host compliance reporting via network configuration, allowing global risk assessment and formulation of profitable mitigation strategies. To quantify corporate risk on a worldwide scale, the authors established particular measures based on the vulnerabilities in network assets, their settings, and their interdependence. This approach represents a critical step forward to automated security hardening through the use of the newest open standards, including the Security Content Automation Protocol (SCAP).

Shackelford et al. [86] conducted brief research on firms based in the United Kingdom and the United States of America that operate in the Medical, Finance, Energy, and Chemical industries. Risk is quantified using a mathematical calculation provided by Judge Hands. They have determined that NIST is the appropriate approach.

Sommestad et al. [87] compared industry-accepted standards for the construction of SCADA systems. The authors offer a mechanism for evaluating these requirements using a ranking system. They

found that ISO/IEC 17799 is more of a management activity security standard.

Azuwa et al. [88] presented a methodology for evaluating an institution's network security management efficiency. Additionally, the authors discussed how to calculate risk in company management using the Plan-Do-Check-Act (PDCA) approach.

Saleh et al. [89] developed a model based on Strategy, Technology, Organization, People, and Environment (STOPE) principles and a mathematical model for evaluating the organization's standards and practices and comparing them to ISO standards in order to identify their degree of compliance with ISO/IEC 27001.

Almuhammadi, Sultan, Alsaleh, and Majeed [90] conducted a study of current maturity models and found that no independent and unified maturity model exists for the NIST Framework. As a result, the authors suggested their maturity model for the NIST cybersecurity framework in order to analyze and assist in developing the information security system's development plan.

L. Cyra et al. [91] developed the Standards Conformity Framework (SCF), a framework that establishes a generic template for conformance with various standards, including Common Criteria v2.2, ISO 14971, BS 7799-2, ISO/IEC 27001, and ISO/IEC 15408. It is possible to extract specifications from standards and their accompanying documentation. They developed a tool called TCT that can be used to generate a template from a certain standard.

Livshitz et al. [92] highlighted the difficulties associated with implementing an information security management system (ISMS) to assess the conformity of electronic services (ES). Numerous issues arise in businesses that deal with ES. In the ES providing sector, international guarantees can be given utilizing a variety of ways. The performance evaluation of the ES infrastructure as an ISMS and the issuing of an ISO 27001 compliance certificate ensures the acceptance of belief by all parties in the information exchange process.

A thorough summary of previous research efforts is summarised in Table 4.1. In the subsequent subsections, we individually evaluate the selected cybersecurity standards and current software tools employed by different industries.

Table 4.1: Related Research Work

Author	Year	Standard	Domain	Remarks
--------	------	----------	--------	---------

Teodoro et al. [76]	2015	NIST	Cybersecurity	Model measures existing cybersecurity threats, assign monetary investment values towards explicit compliance intentions, and decreases any existing resource overlapping.
Giulio et al. [77]	2017	Generalized	Cloud Security	Focuses on general IT Security by providing in-depth analysis of standards alongwith some recommendations.
Duncan et al. [78]	2014	Generalized	General IT Security	Provides a comprehensive analysis and comparison of standards in terms of their evolution, identified improvements and flaws that need to be addressed, but it only focuses on general IT security
Piromsopa et al. [79]	2017	PCI DSS, HIPAA, ISO 27001	Insurance Industry	Proposes a scoring model for cyber insurance based on internal and external audits and compliance with mandatory and voluntary standards. The scoring model is based on compliance with the necessary standards, i.e., PCI DSS, HIPAA, SOX, Basel, and ISO 27001.
Pardo et al. [80]	2012	COBIT, ISO 27002	Generic	Presents a formalized approach for deriving related concepts and commonalities in different models. A web-based tool is presented that has been put into practice to unify different models, namely COBIT [89], Basel II, RISK IT, VAL IT, ITIL, and ISO 27002.



Pardo et al. [82]	2010	Generalized	Generic	Stresses on the significant difference within the components, terms, and procedures that impede the unification of various models.
Mellado et al. [83]	2007	Common Criteria	General IT Security	Introduces a process based on different Common Criteria (CC) constructs named Security Requirements Engineering Process (SREP).
Li et al. [84]	2015	ISO/IEC27001	Information Security	The model uses a questionnaire-based approach on 133 controls of ISO/IEC27001 standard to collect responses from IT professionals about the security Information Security Stresses on the significant difference within the components, terms, and procedures that impede the unification of various models.aspect of virtualization.
Alsaleh et al. [85]	2016	OpenSCAP	System Security	This model is a vital step towards automated security hardening by utilizing the latest open standards, i.e., Security Content Automation Protocol (SCAP).
Shackelford et al. [86]	2015	NIST	Medical, Finance, Energy	Presents a brief study on the UK and US-based companies from Medical, Finance, Energy and Chemical industry domains. A mathematical equation given by Judge Hands is used for the evaluation of risk.

Sommestad et al. [87]	2010	ISO/IEC 17799	Industrial Security	Presents a ranking based model for the evaluation of these standards. They have concluded that ISO/IEC 17799 is more of a security standard for management activities.
Azuwa et al. [88]	2012	Generalized	Network Security	Proposes a model to assess the efficiency of network security management in any organization. They also presented a Plan- Do-Check-Act (PDCA) model for the calculation of risk in business management.
Saleh et al. [89]	2007	ISO/IEC 27001	Information Security	The model is based on Strategy, Technology, Organization, People, Environment (STOPE) along with a mathematical model to evaluate the organization's employed standards and practices and benchmark them with ISO standards to determine their level of compliance with ISO/IEC 27001.
Almuhammadi et al. [90]	2017	NIST	Cybersecurity	Reviewed existing maturity models and concluded that there does not exist any standalone and single maturity model for NIST Framework.
L. Cyra et al. [91]	2011	CC, ISO/IEC 27001	Information Security	Introduced a Standards Conformity Framework (SCF), which creates a generalized template for conformity with various standards such as Common Criteria v2.2, ISO 14971, BS 7799- 2, ISO/IEC 27001, ISO/IEC 15408.

Livshitz et al. [92]	2012	ISO 27001	Information Security	Discusses challenges in implementing an information security management system (ISMS) for the compliance evaluation of electronic services (ES).
----------------------	------	-----------	----------------------	--

## 4.2 Existing Security Standards

For the protection of computer systems, several cybersecurity standards have been defined. Numerous organizations are mandated with the duty of developing standards, industry-wide norms, and laws. To provide optimum security and risk minimization, organizations like NIST, ISO, FIPS, and CC have created their respective frameworks and collection of cybersecurity standards. These standards are exhaustive in their coverage of enlisted configurations. We should collect all specifications and configurations associated with a single functioning machine while limiting our focus to OS-related requirements. Each criteria under consideration are discussed in full below.

### 4.2.1 National Institute of Standards and Technology (NIST)

NIST is a division of the United States Department of Commerce. This body exists only to govern new industry standards and to identify improvements. It was founded in 1901 and has since established standards for a variety of sectors. It is based in Gaithersburg, Maryland, and operates six laboratories: the Communication Technology Laboratory, the Engineering Laboratory, the Information Technology Laboratory, the Neutron Research Center, the Physical Measurement Laboratory, and the Material Measurement Laboratory. President Obama authorized money for the creation of cybersecurity standards in 2013. Following a series of early workshops in 2013, the first publication of Cybersecurity standards was made available in 2014. The framework was improved in response to ongoing comments and developments in practical technology, and three more modifications were issued in the following years [93].

The specification is divided into three sections: Framework Core, Implementation Tier, and Framework Profiles. The Core of Framework consists of five stages: identification, protection, detection, response, and recovery. Organizations must follow these measures when it comes to risk management. Tier-1 through Tier-4 implementations correspond to the level of security controls and parameters that an organization demonstrates by implementing the required features in the appropriate tier. The Framework Profile is a collection of specific requirements, i.e., those that must be implemented exactly as specified in the standard. NIST standards are classified according to their significance.

NIST has a total of eighteen (18) classifications. Each category has its own set of standards, which are classified according to their importance. The standard has one hundred and fifty-nine (159) major categories, which are divided into eleven (11) divisions. The access control category consists of twenty-five (25) major categories. Several subcategories related to Auditing and accounting are classified into sixteen (16) categories and several subcategories, including criteria for audit events and non-repudiation guarantee. Five (5) areas and several subcategories comprise the criteria for security awareness and training of an organization's workers. Configuration management is divided into eleven (11) areas with several subcategories. These categories include criteria for a random set of controls such as installed software, minimum functionality, access restriction, and effect analysis. The contingency plan is divided into thirteen (13) sections and several subcategories, including criteria for preparation, backups, and alternate tactics. Identification and Authentication have eleven (11) primary categories and several subcategories, including needs for authentication rules and policies, device and user identification, etc.

Incident Response is divided into ten (10) major areas with several subclasses that include incident-related tasks, such as planning, handling, monitoring, and reporting. Maintenance is classified into six (6) major areas and several subcategories that included requirements for the maintenance schedule, policies, processes, etc.

Media protection is divided into eight (8) major areas and several subcategories, including regulations for media protection, access, storage, transit, and use. Personnel Security is divided into eight (8) major areas and several subcategories that include monitoring, termination, and transfer. Physical and Environmental Prevention is divided into twenty (20) categories and several subcategories. These categories include standards for physical device security, visitor logs, and arson and flood damage protection. Planning is divided into nine (9) categories and several subcategories, each of which has its own criteria. Program management is divided into sixteen (16) major areas and several subcategories. These categories include requirements for risk management, system inventory, testing, and danger awareness programs, among others. Six (6) areas and several subcategories comprise risk assessment, including criteria for risk appraisal in diverse situations and vulnerability screening. Security Assessment and Authorization are divided into nine (9) categories and several subcategories, including penetration testing, security certification, and security assessment. Systems and Communication Protection is divided into 44 categories and several subcategories, most of which are concerned with network-based security settings. System and Information Integrity is divided into seventeen (17) categories and several subcategories, each containing criteria relating to the system's correct operation safely and securely. System and service acquisition is divided into twenty-two (22)

major categories and several subcategories, each with its own set of criteria for external resource use and security limitations.

#### **4.2.2 Federal Information Processing Standards (FIPS)**

FIPS is a collection of encryption standards established by the United States Federal Government. FIPS is a non-military standard developed to assure data security and connectivity across government agencies, suppliers, and contractors. The majority of the controls in FIPS are variants of those found in the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO). These standards are extensively utilized by a variety of organizations worldwide. FIPS standards are established descriptively for public usage to provide optimum security, reliability, and integrity of the system [94]. The standard is arranged in four distinct levels with respect to the level of security controls that need to be applied with the expense for implementation. Starting from Level 1 to Level 4, it provides a varied configuration that anybody may employ as per their demand and finances. The standard provides the correct amount of security settings to maintain the system's integrity, covering from physical security to the low-level configurations in the network and the transport layer of network communication. Organizations are recommended to utilize hardware devices having FIPS encryption configured.

#### **4.2.3 ISO/IEC 27001-2**

The International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) are both international organizations that are jointly working with various countries (164 approx.). It was founded in 1947 and is based in the Swiss city of Geneva [95– 97]. Over the years, ISO has created standards for a variety of industries. Initially, ISO/IEC released ISO/IEC 17799 in 2005 for security and risk management. The security requirements were later improved and standardized as ISO/IEC 27001/2. ISO/IEC 17799 is geared at organizational management, whereas ISO/IEO 27001/2 is more comprehensive in terms of technical and practical issues of implementing security controls for securing digital assets.

#### **4.2.4 Common Criteria (CC)**

Common Criteria (CC) was created in partnership with six countries: Canada, the United States, Germany, France, the United Kingdom, and the Netherlands [98]. CC is an ISO/IEC standard 15408 for computer security that places a greater emphasis on the assessment of the final work product during the testing process than other standards do. There is an OS Protection Profile that has numerous improved standards for hardening the OS's security. The CC standards were derived from three

previous standards, namely the Information Technology Security Evaluation Criteria (ITSEC), the Trusted Computer System Evaluation Criteria (TCSEC), and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC). ITSEC was a European standard established in the 1990s with the assistance of the United Kingdom by France, Germany, and the Netherlands. CTCPEC was initially released in 1993 and was utilized jointly by the United States and Canada. The US Department of Defense created TCSEC in the 1970s and 1980s.

CC was developed through the process of improving the current set of rules derived from the previous standards. Table 4.2 compares NIST, FIPS, ISO, and CC standards in terms of the requirements for a single PC's operating system. We evaluated this standard in many areas, including User Accounts and Access Policies (UAAP), Networking, Cryptography, Logging/Auditing, Physical/Hardware, Triggered Notifications, and Authentication.

Table 4.2: Security Compliance Standards and Supported Controls

Name	Year	UAAP	Network	Cryptography	LA	PH	NTE	Authentication
NIST	2014-Rev-1/2/3/4	✓	✓	✓	✓	✓	✓	✓
ISO	2005-2006	✓	✓	✓	✓	✓	✓	✓
CC	US-2016	✓	✓	✓	✓	✓	✗	✓
FIPS	2001	✗	✓	✓	✗	✓	✗	✓

We have categorized the requirements for user accounts, including temporary accounts and installation rights, under the UAAP category. We examined the use of insecure ports and protocols, RDP, Time Sync, and server and firewall settings under the network category. We have classified cryptography into three categories: encryption of data in motion, encryption of data kept on a local system, and certificate expiration. We evaluated state verification of logging, i.e., whether it is enabled or disabled, the availability of a method to prevent log tampering, i.e., write once read many (WORM), and lastly, log encryption. In the Physical and Hardware (PH) category, we've grouped configurations for physical and portable devices, such as a CDROM or Flash Drive, as well as system hardware information, such as the presence of a backup server. We evaluated broadcast messages to the administrator in the Notification and Triggered Events (NTE) category. We have classified authentication techniques into three categories: single-factor authentication, multi-factor authentication, and minimum-maximum password length and life.

### **4.3 Existing Software Tools**

This section discusses existing tools that aid in the operation of complying with various cybersecurity requirements. Since several of these tools require expensive licenses, conducting real-world testing is not practical. As a result, additional sources such as online websites, user instructions, and third-party evaluations were employed to gather details regarding these products.

#### **4.3.1 Acuity STREAM**

Acuity Strategic Risk-based Enterprise Assurance Management (STREAM) is a comprehensive, highly adaptable, and simple-to-use software solution that streamlines the time-consuming process of complying with numerous standards and ensuring effective risk management [99]. STREAM is a multi-user tool that, through a rule-based approach, facilitates the division of responsibilities. This program is also accessible in the single-user mode for smaller businesses. According to the organization's risk tolerance, STREAM provides actionable information into the present state of compliance with a certain standard and residual risk. The expressive widgets are complemented by a collection of graphical charts that present a more comprehensive view of compliance and level of risk. This tool complies with all applicable security requirements, including NIST, PCI DSS, ISO 27001, and GDPR.

Additionally, it provides real-time information on risk assessment with respect to risk tolerance and compliance status with standards. Additionally, it can track risk mitigation measures and determine how controls influence the residual risk status. Acuity STREAM is available on both Windows and Mac OS platforms.

#### **4.3.2 Vigilant Software(vs) Risk**

vsRisk was designed with the ISO/IEC 27001 standard in mind [100]. It aids in the tracking and administration of assets in accordance with risk assessment. vsRisk is a stand-alone program for small to medium-sized businesses and a multi-user solution for big companies. Additionally, it is compliant with PCI-DSS, NIST, and ISF information security and enables asset-based vulnerability and threat detection, as well as a wizard-based method to speed the Risk Assessment process. Not only does vsRisk have built-in Audit Trails, historical records, and controls compliant with the ISO/IEC 27001 standard, but it also supports the import of controls compliant with additional standards. The program generates six audit-ready reports, including a risk treatment plan and a Statement of Applicability (SoA). The vsRisk application is solely compatible with Microsoft Windows, although a cloud-based alternative is also available for bigger businesses. The cloud-based functionality enables upper management to understand better the whole process of complying with a certain standard.

### **4.3.3 Microsoft Baseline Security Analyzer (MBSA)**

It was formerly referred to as Microsoft Personal Security Advisor (PSA). It examines Windows-based PCs or clusters of Windows-based systems for common security misconfigurations. The MBSA includes a checklist of what was reviewed and recommendations for resolving any faults that were discovered. Additionally, it identifies missing updates and determines if Windows is configured according to industry best practices. It does not adhere to any specific security standard, such as NIST, CC, or FIPS, and solely supports the Microsoft Windows operating system. MBSA generates an XML-formatted report for each computer examined and shows it in a browser window. Not only does the program check for missing hotfixes, but it also scans the status of guest accounts and displays a list of additional accounts with administrator privileges. Additionally, MBSA inspects each disc independently and recommends suitable auditing and logging services and identifying idle services running on the computer.

### **4.3.4 Microsoft Security Assessment Tool (MSAT)**

MSAT performs comprehensive security evaluations, which is only compatible with Microsoft Windows operating systems. This application is intended to provide information and suggestions regarding industry-standard best practices for IT-based infrastructure security [102]. It is aimed at small to medium-sized businesses and includes around 200 questions organized into four main categories: infrastructure, operations, applications, and staff. MSAT draws on various sources, including ISO/IEC 17799, NIST-800, and Trustworthy Computing Group guidelines (TCG). The auditor is supplied with the resulting security assessments, recommendations and mitigation information, and references to more information. MSAT generates reports that detail the business's overall risk and present an index in relation to the security procedures in place. Additionally, it compares the security posture to prior assessments and gives additional guidance on how the present controls function compared to previous security settings. Lower-level security controls use a reactive strategy, whereas higher-level security controls use a proactive approach.

### **4.3.5 Belarc Advisor**

This program enables you to collect data on all the connected devices to your computer [103]. It provides the network configuration and applications installed on the machine. Using the installed software list and Microsoft Windows updates information, it also discovers system security flaws. This software does not resolve these problems but does bring them to the system administrator's attention for remediation. It gives data on the equipment and applications listed along with their associated information, such as serial numbers. Belarc does not adhere to any of the widely accepted



security requirements. It is compatible with both Microsoft Windows and UNIX-based operating systems. Additionally, Belarc recommends which program is not functioning correctly and requiring more troubleshooting.

#### **4.3.6 Lynis**

Lynis is a security assessment application for UNIX-like systems that enable businesses to assess their existing security settings and posture. The tool's core objective is to evaluate a system and offer valuable insights into system hardening [104]. Lynis scans the system in a modular and opportunistic manner; for example, if it identifies that the host has an Apache server, it looks for settings and vulnerabilities unique to that version and assists the administrator in resolving specific concerns. Lynis has several capabilities, including intrusion detection, comprehensive reporting, vulnerability identification, and system hardening. Additionally, it complies with ISO/IEC 27001, PCI-DSS, and HIPAA regulations but is only compatible with UNIX-based systems. Since Lynis operates on the target host, it can gather more information on the system than other analyzers. It is concerned primarily with boot loader files, software programs, configuration data included inside system files, and configuration associated with logging and system auditing. After the system scan, Lynis generates a hardening score. Lynis displays a warning and a suggested remedy for each security flaw discovered.

#### **4.3.7 Open Security Content Automation Protocol (OpenSCAP)**

The OpenSCAP tool was created to assess an organization's overall security by establishing a security baseline [105]. OpenSCAP includes several built-in features, including system configuration scanning, vulnerability scanning, Security Content Automation Protocol (SCAP) validation, and detecting whether the computer has been hacked. OpenSCAP protects against intrusions and provides thorough reporting. It complies with SCAP and PCI DSS security requirements which are only compatible with Linux operating systems. Extensible Configuration Checklist Description Format is used by OpenSCAP (XDCCDF). It is a combination of many existing specifications, including Common Configuration Enumeration (CCE), Common Platform Enumeration (CPE), and the Open Vulnerability and Assessment Language (OVAL).

#### **4.3.8 Tiger**

Tiger is a security auditing and hardening program that is used to determine which current updates are not installed, file system privileges, inactive users, intrusion detection, and vulnerability scanning, among other things. Tiger verifies system settings and the current state of the system [106]. It displays options and recommendations to strengthen further the present system's security based on

the collected data. It is compatible with any UNIX-based system. Once the scan process completes, the result file is stored on the scanned system as `/var/log/tiger/security.report.mint.YYMMDDHH:MM` and is only readable by admin.

#### 4.3.9 Center for Internet Security (CIS) Configuration Assessment Tool

The CIS Configuration Assessment Tool is a vulnerability assessment tool that scans the target system, identifies vulnerabilities, and verifies that the system adheres to the benchmark of the C.I.S. [107]. If it deviates from the benchmark settings, it offers support for system hardening appropriately. Though reporting is given against several different standards, none of the industry’s mainstream standards are supported. It generates a report with a score between 0 and 100 and correction actions in the event of non-conformance with the benchmarks. A higher score indicates greater compliance with CIS standards and hence a more secure system against attacks.

Table 4.3 summarises the available software tools. A list of software products is supplied, together with data on the operating systems they run, the security standards they adhere to, the graphical user interface, and their portability. While many tools are available, the majority of solutions aimed at OS conformity only support UNIX-based systems. There have been no free portable solutions available for MS Windows OS that adhere to NIST, FIPS, CC, and ISO security requirements. A detailed description is provided above, focusing on the latest research and security requirements in the context of operating systems.

Additionally, the details of available software solutions regarding OS security and their conformance with specific security standards are presented. Each of the security standards includes a list of categories about the operating system. Additionally, there is little overlap between the requirements of every standard. On the other hand, we discussed the features of various applications and their compliance with security standards in existing software solutions (s). Certain tools do not adhere to any security standard and instead focus on providing a general hardening of the system. The majority of tools are available for free, although a few solutions provide a premium version as well. One critical point to keep in mind is that the majority of these tools are not portable.

Table 4.3: Existing Software Tools with Supported Security Standards and OS

Software	IS Standards	Supported OS	License	GUI	Portable
----------	--------------	--------------	---------	-----	----------

Acuity STREAM	ISO 27001, NIST	Windows, Mac-OS	Free	Yes	No
vsRisk	ISO 27001, PCI DSS	Web based solution	Paid	Yes	No
MBSA	Generalized Hardening, NIST	Windows	Free	Yes	No
MSAT	ISO 17799, NIST	Windows	Free	Yes	No
Belarc Advi- sor	Generalized Hardening	Windows, UNIX based systems	Free, Paid	Yes	No
Lynis	HIPAA, ISO 27001, PCI DSS	UNIX based systems	Free	No	No
OpenSCAP	NIST, PCI DSS	Linux	Free	Yes	No
Tiger	Generalized Hardening	Linux	Free	No	No
CIS CAT	Generalized, Internet Security	Windows, UNIX based systems	Free, Paid	Yes	Yes

## **CYBERSECURITY FRAMEWORKS**

While we explored the Cybersecurity standards such as NIST, ISO, CC, and FIPS, we decided to explore the implementation frameworks for these standards further. We discovered the implementation frameworks for NIST, ISO, CC, and FIPS cybersecurity standards. These frameworks present businesses with a set of instructions for implementing the needed standard properly, efficiently, and cost-effectively. Each company has its own set of levels, policies, and processes that must be followed. The following subsections provide a framework associated with each of the information security standards.

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

All requirements, irrelevant to their grouping, are classified into low, moderate, and high severity levels, designed to convey the requirements' relevance. NIST has developed a cybersecurity framework (CSF) comprising industry-standard principles and cost-effective techniques for implementing security controls [108–110]. NIST's framework is divided into three distinct components, as depicted in Figure 5.1. These components are the Framework Core, the Implementation Tier, and the Framework Profile. Each of these is discussed in detail below.

#### **5.1.1 Core**

The Core of Framework consists of five (5) distinct stages. These stages give a high-level overview of the risk management lifespan of an organization and must be followed for risk management objectives. Organizations must establish an enterprise-wide knowledge of cybersecurity risk management during the 'identity' phase, which includes communicating and linking risk with organizational assets such as personnel, systems, and data. The second phase, titled 'Protect,' requires developing and implementing a safeguard plan to assure the safe delivery of important events and services. In the third phase of the Detect procedure, well-planned actions are created and implemented to monitor and detect cybersecurity incidents. The fourth phase, dubbed 'Respond,' defines and implements a series of exercises to be used in the event of a cybersecurity crisis. Finally, in the fifth phase, dubbed 'Recover,' a collection of actions is defined and implemented in order to restore the system to its normal condition in the event of a cyber-incident with the least amount of time and expense.

### **5.1.2 Implementation Tier**

The Implementation Tier embodies the company's perspective on processes and risk management, i.e., how the organization views the security of its processes and the importance of risk management. Tiers of implementation are classified as Partial, Risk-Informed, Repeatable, and Adaptive. Each tier describes the company's level of detail in comparison to the features of standard controls. The Framework profile is a collection of distinct individual criteria that must be fulfilled in accordance with the standard.

In Tier-1, risk management processes are not automated or formalized, and the institution's business objectives and risk objectives are not specified. Additionally, employees are unaware of cybersecurity threats. Any risk management plan is implemented exclusively based on information obtained from independent sources.

Tier-1 is typically applied in areas where businesses lack a clear understanding of their market position and have no demonstrable accomplishments in the field of cybersecurity risk management.

Tier-2 risk management rules are more developed but not yet adopted as a standardized set of procedures across the company. While the organization's staff are informed of cybersecurity threats, a realistic strategy for risk management has not yet been implemented. Employees are informed about cybersecurity risks on a casual and unplanned basis. Rare, ad hoc evaluations are also conducted without regard for a schedule. The company knows its market position and is somewhat reliant on external sources, but it creates its information for risk management. Additionally, the company is aware of the risks connected with its services and clients but does not adhere to standards formally.

Tier-3 organizations have well-organized and structured their cybersecurity policies, processes, and set of tasks. The plans are updated and maintained in accordance with the most current technology landscape and organizational requirements. Policies and duties are clearly established and executed, as is the routine practice of reacting to every system event or change. Risk monitoring is conducted efficiently, and all top people in the business interact routinely and on a planned basis on cybersecurity risk management. Cybersecurity and risk management are given appropriate weight in corporate activities. The organization is aware of its position and related risk in the industry and with stakeholders. The organization contributes appropriately to the community and provides information with other partners to improve its operability. Additionally, it understands the risk connected with its services, products, and clients and generally works in accordance with established standards, procedures, and a structured environment.

The tier-4 organization is responsible for continuously updating and enhancing corporate risk man-

agement policies based on past experiences and projections. Strategies and actions are reviewed and changed regularly to reflect changes in the technology landscape and adapt to changing organizational demands. Policies, risk management events, and operations are established, implemented, and well-practiced on an institutional level. The senior managers fully identify and understand the underlying link between business goals and cybersecurity. Cyber threats are ranked on a par with financial risks. Risk management procedures are developed enough to quantify the risk attached with a scenario, and senior managers recognize tolerance for risk while making decisions. Employees in the organization are sufficiently trained to accurately assess the cybersecurity risk associated with certain news events and respond appropriately. The organization is aware of all stakeholders, including dependents and dependencies, and makes a major service to the organization. They do real-time monitoring, ongoing evaluation, and prioritizing of risk management activities. Sophisticated threat management approaches, such as advanced persistent threat elimination, are adapted. Motives and objectives of the organization are well-managed in light of the current technology landscape.

### **5.1.3 Framework Profile**

A framework profile is a collection of coherent criteria that an organisation produces in response to its existing implemented cybersecurity profile and compares it to its intended cybersecurity profile. The framework profile identifies the enhancements that must be addressed to reach the required level of cybersecurity. To build the profile, companies must regularly examine all categories to decide which controls should be included in the target profile. These profiles are reviewed and changed as necessary to manage organizational risk.

Additionally, the framework profile represents the organization's risk management approach, which is consistent with regulatory requirements, organizational needs, and objectives. The organization's present profile details the cybersecurity approaches and settings in place, whereas the goal profile details the requirements that must be met. If a discrepancy between the existing and target profiles is discovered. In that case, risk management-based measures are advised to attain the necessary degree of security in the most cost-effective manner.

## **5.2 CC Cybersecurity Framework**

Common Criteria is a framework of itself, allowing users to specify their preferred levels of security and assurance. Vendors can implement required security by utilizing protective profiles or selected components. Claims can be validated by auditing companies that conduct compliance assessments of other businesses, services, and goods against worldwide standards. For instance, CC requires establishing and assessing a management system [111], [112]. To be recognized as CC compliant,

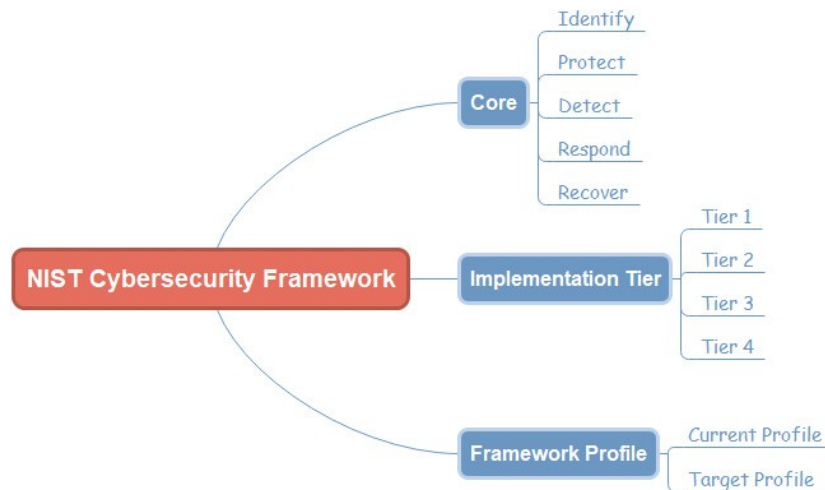


Figure 5.1: NIST Cybersecurity Framework

the created product must be examined by a laboratory. Figure 5.2 illustrates keywords and ideas associated with the creation and assessment of CCs.

### 5.2.1 Target of Evaluation

The evaluation target is the equipment that is to be examined or analyzed.

### 5.2.2 Protection Profile (PP)

PP is a document prepared by users or suppliers to satisfy all of their product's security needs. Security objectives, assumptions, security-related functional requirements, security weaknesses, and assurance requirements form the protection profile. Additionally, PP provides the generic assessment criteria, which serves to validate the vendor's claims. Additionally, PP is used to assess the amount of evaluation assurance utilized to determine the thoroughness of a product's testing.

### 5.2.3 Security Target

It is a document that contains details on the security standards that TOE complies with. The security target may simultaneously assert compliance to several protection profiles.

### 5.2.4 Security Functional Requirements

This document contains all of the required security requirements that should be included in the product. This document consists of a list of all security-related functions and their associated objective dependencies. This document is sufficiently thorough in containing a description of authentication for each organizational role.

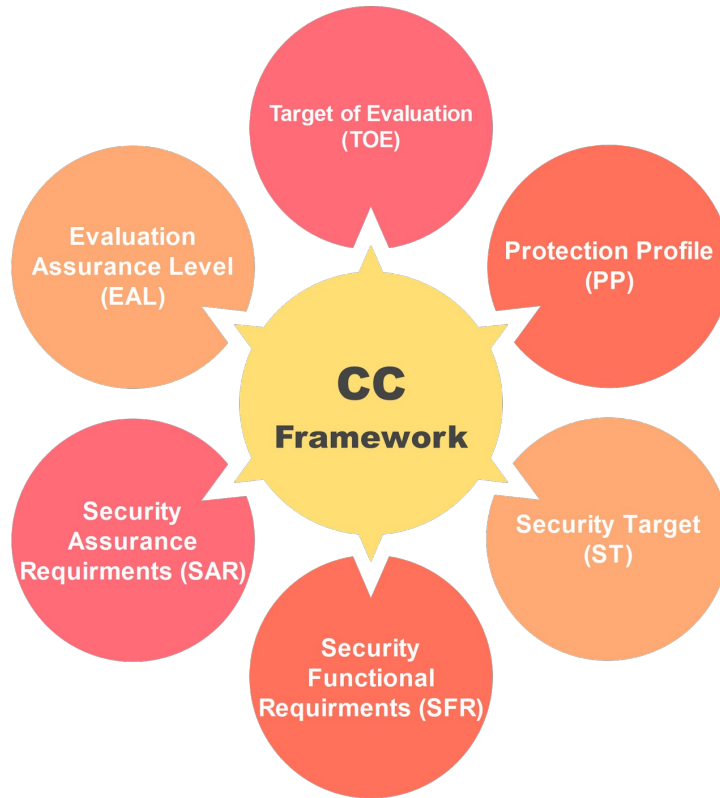


Figure 5.2: CC Cybersecurity Framework

### 5.2.5 Security Assurance Requirement

This document contains all the information on the processes followed throughout the product’s development and assessment for compliance with the standard.

### 5.2.6 Evaluation Assurance Level

This is the numerical rating of the testing phase, which indicates the scope of testing conducted on the product. It is a numeric value between 1 and 7, with 1 showing the lowest degree of testing performed on a product and 7 indicating the maximum amount of testing performed on a product.

## 5.3 ISO Cybersecurity Framework

The International Standards Organization’s cybersecurity architecture is meant to assure security by defining security standards, implementing them, monitoring systems, and continuously improving security. As a result, an organization’s Information Security Management System (ISMS) is deemed to be operational. Additionally, it is believed that the ISMS must adhere to all security and compliance standards [113], [114]. Security-wise, the ISMS is accountable for the confidentiality, availability, and integrity of the organization’s systems.



ISO has created several standards for a variety of sectors since 1947. Due to the extensiveness of ISO standards and the acceptance of numerous standards by complying companies, the issue of conflicting overlapping requirements and challenges and misunderstandings in implementation was highlighted. The majority of businesses use several management systems, which complicates their integration efforts in various ways. As a response, ISO developed the Annex SL Framework, a standardized management system that integrates multiple requirements from different standards and demonstrates exceptional effectiveness throughout implementation. Annex SL has been implemented in conjunction with the following standards.

- ISO 9001:2015
- ISO 14001:2015
- ISO/IEC 27001/2
- ISO 45001:2018

As indicated in Figure 5.3, there are ten stages in the life cycle of Annex SL, which are explained below:



Figure 5.3: ISO-IEC Cybersecurity Framework

### 5.3.1 Scope

The organization defines the requirements for the system's implementation, maintenance, and upgrade in this stage. The criteria set at this stage are irrespective of the organization's size, structure, and type.

### **5.3.2 Normative References**

A document is created that includes information on the relevant standard and a list of requirements that must be implemented with the system.

### **5.3.3 Terms & Definitions**

A formal document is created to handle all relevant terms and conditions in a formal context, for example, legal, technical terms.

### **5.3.4 Context of the Organization**

This stage requires the company to create a thorough document outlining the internal and external challenges affecting the organization's goals and the degree and capabilities of the organization to accomplish the intended outcomes. The company should identify all parties with interest in the organization's requirements, goals, and security and the necessity to define the management system's scope.

### **5.3.5 Leadership**

The upper executives have a pivotal role to play in this phase of the system's development. They should assure the availability of resources and the management system's effective integration into organizational operations. Additionally, top management is accountable for formulating policies and procedures that aid the management system in all aspects. The administration should be ready to communicate with both internal and external entities at all times. Duties and responsibilities should also be allocated, and senior management should guarantee that a suitable reporting process is in place. It has a comprehensive collection of policies that management must apply.

### **5.3.6 Planning**

The operation process involves most of the objectives that must be handled throughout the system's implementation. The management system's progress is monitored and tracked continually to ensure that it proceeds as intended and that any modifications are accommodated in case it is needed. The organization is responsible for guaranteeing the system's correct operation during the planning stage, including identifying and resolving all risk scenarios and possibilities. Management is accountable for refining objectives and developing plans to achieve them. In this stage, risks identified in previous phases must be handled and planned for appropriately. A special emphasis is focused on precisely defining the management system's goals.

### **5.3.7 Support**

The organization identifies several activities in this stage, including resource identification, competency development, awareness programs, communication, and documentation of previously identified information. The data obtained in the previous phases is utilized to determine all possible support goals and objectives. Internal and external communication and any documented material are categorized and arranged in preparation for the next stage.

### **5.3.8 Operation**

The operation process involves most of the objectives that must be handled throughout the system's implementation. The management system's progress is monitored and tracked continually to ensure that it proceeds as intended and that any modifications are accommodated in case it is needed.

### **5.3.9 Performance Evaluation**

The organization is responsible for determining where, how, and when monitoring, analysis, and evaluation will take place. Additionally, an internal audit is conducted to confirm that the built system meets the organization's needs while adhering to the standard's criteria. The system's successful installation and maintenance are benchmarked, and the management system's effectiveness, appropriateness, and fit for organizational needs are evaluated.

### **5.3.10 Improvements**

Finally, the company determines all non-compliant obligations and the measures required to mitigate their risks. The organization is accountable for enhancing strategy in response to the rapidly changing commercial and technology context.

## **5.4 FIPS Cybersecurity Framework**

The FIPS-140 series is intended for security modules that are both hardware and software-based. Both FIPS-1 and FIPS-2 were designed to tighten security and are classified in such a manner that the series code identifies the specific module, such as hardware, software, name, firmware, and version. FIPS-2 [115] is the second release in the series. It contains modifications made in response to user feedback and based on the requirements of the previous version of the standard, FIPS-1. The FIPS standard promotes data encryption. As indicated in Figure 18, FIPS Security Levels define the security criteria that must be executed in an organization.

### **5.4.1 Level 1**

Level 1 provides the minor layer of protection by utilizing at least one authorized algorithm. At this level, physical security is not addressed. Typically, this is accomplished at the software level,

i.e., the application layer, through secure protocols such as TLS to encrypt data during transmission and storage. This software-based approach is far more cost-effective than other hardware-based data security techniques; it also gives a range of cryptographic algorithm selection options.

### 5.4.2 Level 2

It strengthens security further by including restrictions such as tamper resistance in addition to level 1 security. Certain physical limitations are necessary to guarantee the cryptographic components in the system are protected. A physical sealing, coating, or covering must be used to secure the component from tampering. At this level, a role-based authentication approach is proposed, in which the concerned individual is assigned the role of using the cryptographic module exclusively within the organization.

### 5.4.3 Level 3

Level 3 strengthens the security of previous levels by introducing restrictions that prohibit an attacker from obtaining access to cryptographic modules' Critical Security Parameters (CSP). It consists of highly accurate and comprehensive cryptographic module tampering detection. Cryptographic components operate by converting plaintext input to ciphertext output. Once tempering is identified, the cryptographic module's plaintext is deemed null and invalid.

Table 5.1: Categories of Proposed Set of Requirements

Category	Description
User Accounts and Access Policies	Requirements are related to user accounts, including temporary accounts.
Network	Usage of insecure ports and protocols, time sync and firewall configurations.
Cryptography	Traffic encryption in transit, data stored locally and certificate expiry, etc.
Logging/Auditing	The state of logging, logs encryption, mechanism to avoid log tempering, etc.
Physical/Hardware	Configurations of portable devices, hardware details, backup server, etc.
Triggered Notification	The broadcast message to the administrator.

Authentication	The authentication mechanisms, length of password, password life etc.
----------------	---

#### 5.4.4 Level 4

Level 4 security solution satisfies all security criteria in the preceding three modules and the need for prompt identification and removal of all leaked plaintext data. Security level 4 modules combine the functionality of previous levels with the ability to operate outside of a physically secure environment since they incorporate more crucial and effective detection methods for physical access than level 3 components. Security solution satisfies all security criteria in the preceding three modules and the need for prompt identification and removal of all leaked plaintext data. Security level 4 modules combine the functionality of previous levels with the ability to operate outside of a physically secure environment since they incorporate more crucial and effective detection methods for physical access than level 3 components.

FIPS-compliant implementations include ports, interfaces, services, authentication and responsibilities, a deterministic finite model, physical security, the operational environment, cryptographic key management, electromagnetic interference, self-tests, and architectural assurance. A cryptography module may be physical, software, or firmware in nature. Physical characteristics vary according to the kind of cryptographic module employed, from physical confinement, such as locks and doors, to the process being kept in tamper-proof memory, which provides security of the processor and all other essential physical hardware.

## **PROPOSED FRAMEWORK FOR WINDOWS**

To deal with the challenges identified during the existing literature and provide structured to operating system security assessment, we propose a framework that is simple and flexible for end-user as well as system administrators to implement which does not require any advanced human skill or any other tool. Additionally, this technique sets minimum security criteria based off of globally recognized standards, which ensures the quality of the process's complete security review.

The security of the operating system must be tested as its use at household or in organizations, as the majority of the time, the inbuilt security measures of the operating system are not applied effectively by the end-user, or perhaps the end-user is ignorant of the security misconfigurations on their personal computer. As a result, to safeguard Windows 10 end-users from unauthorized access to sensitive data, we developed a security compliance framework that addresses all of their security issues and not only assesses the Windows 10 OS's security against universally recognized criteria but can also be used by any end-user regardless of size of organization or type of job. The suggested Windows 10 security compliance framework's critical stages are illustrated in Figure 6.1 and discussed in detail throughout the remainder of this chapter.

### **6.1 Proposed Framework Steps**

Six phases must be followed in order to evaluate the security of the Windows 10 operating system. Each phase is detailed as follows:

#### **6.1.1 Security Controls**

This phase establishes the security standards criteria that will be used to assess the Windows 10 operating system. For this purpose, we have selected NIST SP 800-53, which is not intended particularly for OS security, we evaluated the security control types which can be seen in Table 6.1. We selected security controls which were most appropriate for Operating System security assessment. The information gathered in this phase will be utilized to evaluate the framework's subsequent stages.

Table 6.1: Security Controls

Identifier	Family	Number of Security Controls	Number of Selected Security Controls	Selected Security Controls
AC	Access Control	25	5	AC-2;AC-6;AC-7;AC-9;AC-17
IA	Identification and Authentication	12	2	IA-3;IA-5
SI	System and Information Integrity	23	3	SC-28;SC-41;SC-18
SC	System and Communications Protection	51	3	SC-28;SC-41;SC-18
CM	Configuration Management	14	6	CM-2;CM-3;CM-7;CM-8;CM-10;CM-11
AU	Audit and Accountability	16	6	AU-2;AU-3;AU-4;AU-8;AU-9;AU-14

### 6.1.2 Security Controls Categorization

This phase organizes all of the previously identified security controls into the categories. There are 14 distinct security categories which are regarded critical when evaluating an operating system's security. This classification of security needs into distinct domains facilitates us in comprehending the security areas relevant to operating system evaluation, allowing for a more thorough evaluation methodology.

Table 6.2: Security Controls Categorization

Security Control Categories	Number of Security Requirements	Details
Countermeasures	5	It comprises of Security Requirements for protection against internal and external attacks.

User Accounts	7	It comprises of Security Requirements dealing to the security and administration of user accounts.
Network & Internet	7	It offers Security Requirements for secure network protocols, including WLAN.
Software & Hardware	10	It comprises of Security Requirements regarding hardware and software.
Cryptography	3	It comprises of Security Requirements pertaining to cryptographic methods used in data storage and processing.
Logs	3	It comprises of Security Requirements deals with event log creation and security.
System Settings	5	It comprises of Security Requirements for customized users and the registry.
RDP	2	It comprises of Security Requirements relating to item and resource access control.

### 6.1.3 Evaluate System

This step is critical to our proposed architecture since it is responsible for creating tests to verify the state of each Security Requirement of evaluating system. As mentioned before, the suggested framework should be quickly accepted by users in allowing them to self-assess the security of their operating systems. As a result, this phase focuses on developing testing that are simple to run for non-technical people and do not need the usage of any complicated tools or system configuration. To achieve the same, and avoid using any third party application we have created a simple toolkit which the user can use with simple clicking and doesn't need to type in long commands into power-shell or similar system.

### 6.1.4 Check Compliance

Following the completion of each test, this phase combines and classifies the findings from the previous stage. Once the tests are completed we calculate the result for each security control category, based on the results the assessed operating system is categorised as "Completely compliant," "Partially compliant," or "Non-compliant". Operating systems classified as "Completely compliant" or "Non-compliant" are not subsequently considered. Nevertheless, the following procedures are con-



ducted on “partially compliant” operating systems in order to get their precise compliance score. For partially compliant system each categories score is shown and the categories which have security requirements unmet are shown to user so the end-user can apply security controls to Operating System.

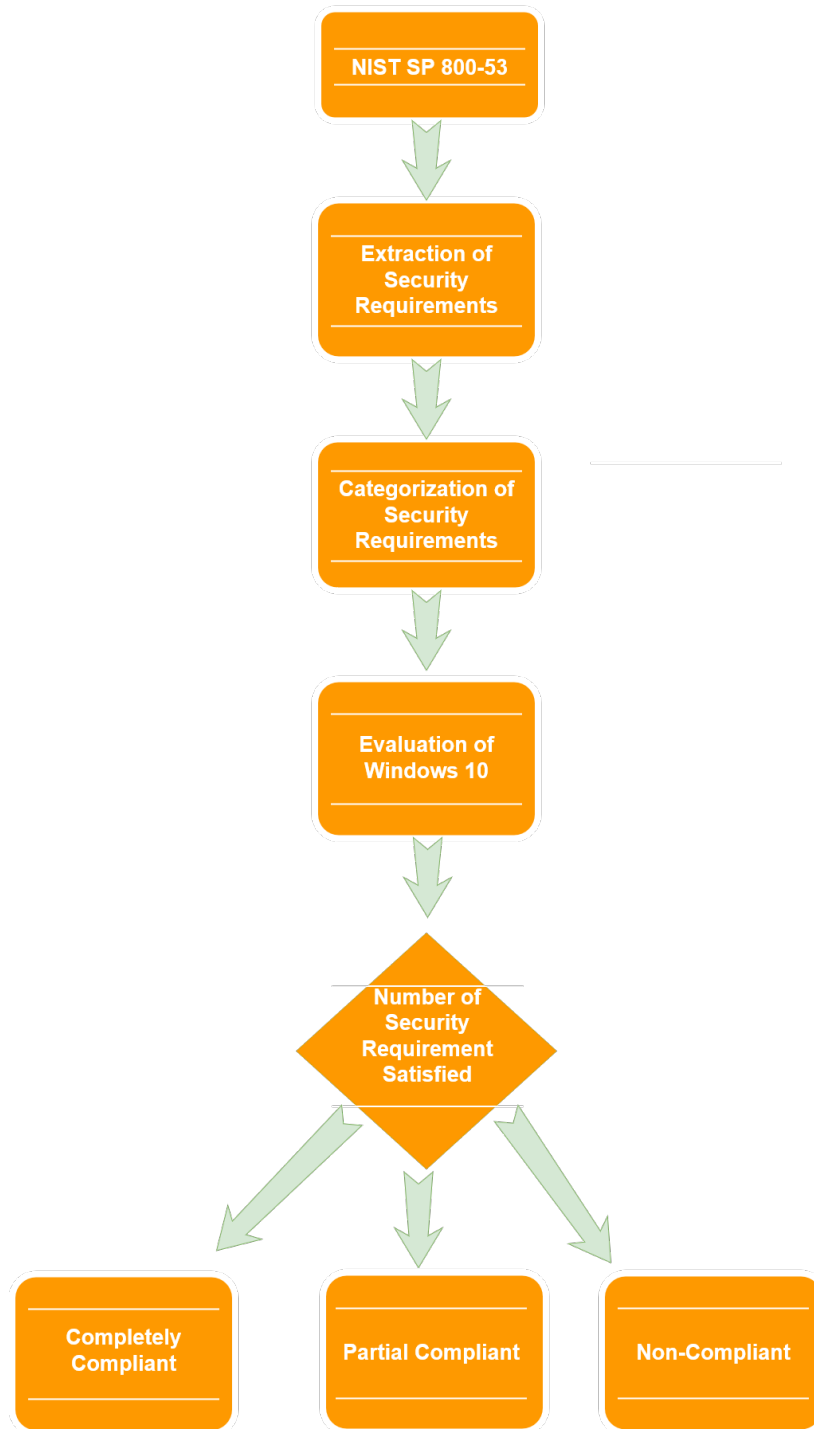


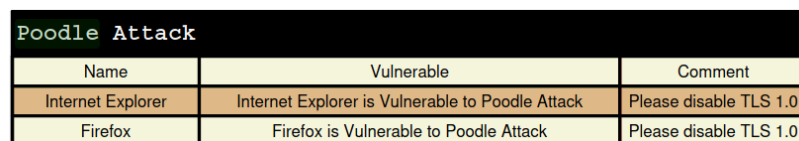
Figure 6.1: Proposed Framework

## VALIDATION OF PROPOSED FRAMEWORK

To validate and demonstrate the proposed framework, we ran it on a desktop running Windows 10. The desktop system is used by 4-5 people so the system has multiple accounts setup. Computers are used to store personal data and to connect internet-based apps including eshopping, banking, entertainment, and download files, among others. As such, security evaluation of an operating system is critical, just just as in any other company or business setting that makes use of computers. We used this framework on a local Computer using the 64-bit Windows 10 Pro operating system.

The results found out that the system was not “Partially compliant”. The security controls which were not in place are as follows and there proof can be seen in the attached screenshots:

- Poodle attack 7.1
- Unsigned software 7.2
- Unsigned drivers 7.2
- Unencrypted drives 7.3
- Logs could be read by anyone 7.4
- Auto run enabled 7.5



Poodle Attack		
Name	Vulnerable	Comment
Internet Explorer	Internet Explorer is Vulnerable to Poodle Attack	Please disable TLS 1.0
Firefox	Firefox is Vulnerable to Poodle Attack	Please disable TLS 1.0

Figure 7.1: Internet Explorer and Firefox vulnerable to Poodle Attack

"e:\software installed\pdf24\pdf\bin\zlib-flate.exe"	"Unsigned"	"8:03 AM 5/8/2021"	"n/a"
"e:\software installed\pdf24\tesseract\tesseract.exe"	"Unsigned"	"1:56 AM 7/23/2021"	"4"
"e:\software installed\pdf24\twain\pdf24-Twain32.exe"	"Signed"	"2:46 AM 8/20/2021"	"n/a"
"e:\software installed\pdf24\twain\pdf24-Twain64.exe"	"Signed"	"2:46 AM 8/20/2021"	"n/a"

Figure 7.2: Unsigned Software

Encrypted Drives		
DriveLetter	Encryption Method	Protection Status
C:	None	Unprotected
D:	None	Unprotected
E:	None	Unprotected

Figure 7.3: Unencrypted Drives

Event Logs Access List		
Logs Name	Restriction Set	Rights
Applicaton	False	
Security	True	Administrator
Setup	False	
System	False	
CxMonsvcLog	False	
Hardware	False	
Internet Explorer	True	O:BAG:SYD:(A;;0x07;;;WD)S:(ML;;0x1;;;LW)
Management	False	
Microsoft Office Alerts	False	
Windows Power Shell	False	

Figure 7.4: Event Logs Access Rights

Auto-Run Configurations		
Drive Type	Auto Run	Action
USB	True	
CD/DVD	True	

Figure 7.5: Autorun Settings

## **FUTURE WORK AND CONCLUSION**

### **8.1 Conclusion**

Cyber attacks have increased significantly in recent years. Organizations take a variety of ways to mitigating cyber risks. While organisations employ cutting-edge security systems and foolproof procedures, numerous known incidents of exploitation have occurred, including WannaCry [116] and Stuxnet [117]. During the construction of organisational architecture, the majority of businesses overlook numerous critical security factors. Numerous frameworks exist for developing information technology solutions that ensure an organization's security. We have compiled a complete list of security-related requirements for organisations who cannot afford to implement various frameworks, e.g. NIST, FIPS, CC, etc., in order to comply with required security standards. These criteria apply to a single operating system's security. Additionally, this research compares existing cybersecurity standards and frameworks in detail. A comprehensive research was undertaken to assess cybersecurity standards from the perspective of a single operating system, namely Microsoft Windows. This research classifies sets of criteria according to widely accepted standards. The framework stated can be used by small to large businesses to adopt and evaluate cybersecurity in their organisation.

### **8.2 Future Work**

It is feasible to expand the scope of our study in the future to also include tests for evaluating other operating systems and to automate the suggested technique for other Operating Systems like Linux and Mac OS and to build a toolkit capable of performing of extracting the system security configuration automatically. This eliminates the possibility of human mistake and more rapidly identifies flaws in existing security configurations.

## BIBLIOGRAPHY

- [1] “Staples: Breach may have affected 1.16 million customers’ cards,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://fortune.com/2014/12/19/staples-cards-affected-breach/>
- [2] R. K. Goutam, “Importance of cyber security,” *International Journal of Computer Applications*, vol. 111, no. 7, 2015.
- [3] Y. Harel, I. B. Gal, and Y. Elovici, “Cyber security and the role of intelligent systems in addressing its challenges,” 2017.
- [4] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.
- [5] G. Pender-Bey, “The parkerian hexad: The cia expanded,” *Žiūrėta*, vol. 5, p. 15, 2016.
- [6] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, “Impact of cyber-security issues on smart grid,” in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*. IEEE, 2011, pp. 1–7.
- [7] J. Blackburn and G. Waters, *Optimising Australia’s Response to the Cyber Challenge*. Kokoda Foundation, 2011.
- [8] L. Bennett, “Cyber security strategy,” *ITNow*, vol. 54, no. 1, pp. 10–11, 2012.
- [9] Microsoft, “Microsoft Security Compliance Manager (SCM),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://systemcenter.ru/scm.en/>
- [10] N. Teodoro, L. Gonçalves, and C. Serrão, “Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements,” in *2015 IEEE Trust-com/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 418–425.
- [11] C. N. Murphy and J. Yates, *The International Organization for Standardization (ISO): global governance through voluntary consensus*. Routledge, 2009.
- [12] P. Mell and T. Grance, “Nist, national institute of standards and technology,” *Definition of Cloud Computing–US Department of Commerce.. Special Publication*, vol. 800, no. 145, p. 2011, 2011.
- [13] CIS, “Center for Internet Security(CIS),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.cisecurity.org/>
- [14] ISACA, “Information Technology–Information Security–Information Assurance (ISACA),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.isaca.org/pages/default.aspx>
- [15] Isaca, I. S. Audit, and C. Association, *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. Isaca, 2011.
- [16] ISF, “Information Security Forum (ISF),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.securityforum.org/>
- [17] ITU, “International Telecommunication Union (ITU),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.itu.int/en/Pages/default.aspx>
- [18] D. M. Oh, “International telecommunication union,” 2010.

- [18] ETSI, “The European Telecommunications Standards Institute (ETSI),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.etsi.org/>
- [19] X12, “X12, Charted by the American National Standards Institute,” [Accessed: 31-Dec-2019]. [Online]. Available: <http://www.x12.org/>
- [20] S. C. McKay and C. J. Piazza Jr, “Edi and x12: What, why, who?” *Serials Review*, vol. 18, no. 4, pp. 7–10, 1992.
- [21] ITIL, “Information Technology Infrastructure Library (ITIL) Guide,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.ibm.com/cloud/learn/it-infrastructure-library>
- [22] T. D. Dabade, “Information technology infrastructure library (itil),” in *Proceedings of the 4th National Conference, 2012*, pp. 25–26.
- [23] IEEE, “Institute of Electrical and Electronics Engineers (IEEE),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.ieee.org/>
- [24] P. A. TO, “Institute of electrical and electronics engineers (ieee),” 2007.
- [25] P. S. S. Council, “Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards.” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.pcisecuritystandards.org/>
- [26] IETF, “Internet Engineering Task Force (IETF),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.ietf.org/>
- [27] P. Hoffman and S. Harris, “The tao of ietf-a novice’s guide to the internet engineering task force,” *Tech. Rep.*, 2006.
- [28] O. Foundation, “Open Web Application Security Project (OWASP),” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)
- [29] ILTA, “International Legal Technology Association (ILTA),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.iltanet.org/home?ssopc=1>
- [30] OASIS-Group, “Advancing Open Standards for the Information Society (OASIS),” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.oasis-open.org/>
- [31] A. Barbir and O. Diplomat, “Organization for the advancement of structured information standards,” 2015.
- [32] CC, “Common Criteria: New CC Portal,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.commoncriteriaportal.org/>
- [33] A. Fekete, “Common criteria for the assessment of critical infrastructures,” *International Journal of Disaster Risk Science*, vol. 2, no. 1, pp. 15–24, 2011.
- [34] A. K. Alharam and W. El-Madany, “The effects of cyber-security on healthcare industry,” in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*. IEEE, 2017, pp. 1–9.
- [36] C.-D. Lee, K. I.-J. Ho, and W.-B. Lee, “A novel key management solution for reinforcing compliance with hipaa privacy/security regulations,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 4, pp. 550–556, 2011.
- [35] D. Lyon, “Making trade-offs for safe, effective, and secure patient care,” *J. Diabetes Sci. Technol.*, vol. 11, p. 446–464, 2017.
- [36] “FFIEC-IT Handbook,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://ithandbook.ffiec.gov/>

- [37] S. A. Elnagdy, M. Qiu, and K. Gai, "Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing," in 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2016, pp. 295–300.
- [38] D. W. Opderbeck, "Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry," *Md. L. Rev.*, vol. 75, p. 935, 2015.
- [39] The cybersecurity regulations healthcare, financial services, and retail industries must know about. [Online]. Available: <https://www.csoonline.com/article/3298962/the-cybersecurity-regulations-healthcare-financial-services-and-retail-industries-must-know-about.html>
- [40] P. DSS, "Payment card industry data security standards," International Information Security Standard, 2016.
- [41] "Pci, "data security standard: Requirements and security assessment procedures,"," 2013.
- [42] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to pci dss compliance," in 2016 IEEE Region 10 Symposium (TENSYP). IEEE, 2016, pp. 65–70.
- [43] A. BARICHELLA, "A comparative analysis between europe and the united states," 2018.
- [44] M. D. Smith and M. E. Pate-Cornell, "Cyber risk analysis for a smart grid: How smart is smart enough? a multiarmed bandit approach to cyber security investment," *IEEE Trans. Eng. Manag.*, vol. vol. 65, no. 3, p. 434–447, 2018.
- [45] K. A. M. H. Cintuglu, O. A. Mohammed and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surv. Tutorials*, vol. vol. 19, no. 1, p. 446–464, 2017.
- [46] S. Sharma, "Cyber security for the defence industry,"," *Cyber Security Review*, online at [http://www. cybersecurity-review. com/industry-perspective/cybersecurity-for-the-defence-industry](http://www.cybersecurity-review.com/industry-perspective/cybersecurity-for-the-defence-industry), 2017.
- [47] B. J. Murrill, E. C. Liu, and R. M. Thompson, "Smart meter data: Privacy and cybersecurity." Congressional Research Service, Library of Congress, 2012.
- [48] World Economic Forum, "The Global Risks Report 2018 - Reports - World Economic Forum," Tech. Rep. [Online]. Available: [http://www3.weforum.org/docs/WEF\\_GRR18\\_Report.pdf](http://www3.weforum.org/docs/WEF_GRR18_Report.pdf)
- [49] "British Airways, "Latest information | Data theft | British Airways."," [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information>
- [50] "MyFitnessPal, "MyFitnessPal Security Information FAQ."," [Accessed: 31-Dec-2019]. [Online]. Available: <https://content.myfitnesspal.com/security-information/FAQ.html>[53] "Ticketfly, "Ticketfly cyber incident information."," [Accessed: 31-Dec-2019]. [Online]. Available: <https://support.ticketfly.com/s/article/41507>
- [51] "MyHeritage, "MyHeritage Statement About a Cybersecurity Incident - MyHeritage Blog."," [Accessed: 31-Dec-2019]. [Online]. Available: <https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/>
- [52] S. Morgan, "Cyber security Ventures, Cybercrime Report, Herjavec Group," p. 14, 2017. [Online]. Available: <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>



- [53] B. KASPERSKY; Levine, “The state of industrial Cybersecurity 2017,” Scientist, no. June, pp. 38–42, 2017. [Online]. Available: <https://go.kaspersky.com/rs/802-IJN-240/images/ICSWHITEPAPER.pdf>
- [54] O. Alhazmi, Y. Malaiya, and I. Ray, “Vulnerabilities in major operating systems,” Technical Report, 2004.
- [55] AV Test, “AV-Test 2017-18,” pp. 1–13, 2018.
- [56] CVE MITRE Corporation, “Microsoft Windows 95 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/112/Microsoft-Windows-95.html?vendor\\_id=26](https://www.cvedetails.com/product/112/Microsoft-Windows-95.html?vendor_id=26)
- [57] “Microsoft Windows 98 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/343/Microsoft-Windows-98.html?vendor\\_id=26](https://www.cvedetails.com/product/343/Microsoft-Windows-98.html?vendor_id=26)
- [58] “Microsoft Windows 98se : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/462/Microsoft-Windows-98se.html?vendor\\_id=26](https://www.cvedetails.com/product/462/Microsoft-Windows-98se.html?vendor_id=26)
- [59] “Microsoft Windows Me : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/1061/Microsoft-Windows-Me.html?vendor\\_id=26](https://www.cvedetails.com/product/1061/Microsoft-Windows-Me.html?vendor_id=26)
- [60] “Microsoft Windows Xp : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor\\_id=26](https://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26)
- [61] “Microsoft Windows Vista : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/9591/Microsoft-Windows-Vista.html?vendor\\_id=26](https://www.cvedetails.com/product/9591/Microsoft-Windows-Vista.html?vendor_id=26)
- [62] “Microsoft Windows 7 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor\\_id=26](https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26)
- [63] “Microsoft Windows 8 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/22318/Microsoft-Windows-8.html?vendor\\_id=26](https://www.cvedetails.com/product/22318/Microsoft-Windows-8.html?vendor_id=26)[67] “Microsoft Windows 8.1 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/26434/Microsoft-Windows-8.1.html?vendor\\_id=26](https://www.cvedetails.com/product/26434/Microsoft-Windows-8.1.html?vendor_id=26)
- [64] “Microsoft Windows 10 : CVE security vulnerabilities, versions and detailed reports,” [Accessed: 31-Dec-2019]. [Online]. Available: [https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor\\_id=26](https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26)
- [65] ZDNet CBS Interactive, “Cybersecurity is broken: Here’s how we start to fix it | ZDNet,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.zdnet.com/article/cybersecurity-is-broken-heres-how- we-start-to-fix-it/>
- [66] The SSL Store, “70
- [67] ImmuniWeb, “Abandoned Web Applications: Achilles’ Heel of FT 500 Companies | ImmuniWeb Security Blog,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.immuniweb.com/blog/FT500-application-security.html#3.2>

- [68] Verizon, “2018 Payment Security Report,” p. 50, 2018.
- [69] “Why No HTTPS? The World’s Largest Websites Not Redirecting Insecure Requests to HTTPS,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://whynohttps.com/>
- [70] TechRepublic, “93% of companies have password rules, but it may not protect them from data breaches-TechRepublic,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.techrepublic.com/article/93-of-companies-have-password-rules-but-it-may-not-protect-them-from-data-breaches/>
- [71] “BULLETPROOF ANNUAL CYBER SECURITY A NOTE FROM THE MD,” 2019.
- [72] Cisco, “Cyber Security and Insurance,” pp. 1–2, 2018. <https://www.cisco.com/c/en/us/solutions/security/cyber-insurance/index.html> [Online].
- [73] NationWide, “Small Business Disaster Recovery Survey Results,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://blog.nationwide.com/news/disaster-recovery-plan-study-results/>
- [74] Thalse Security and Ponemon Institute, “Global Encryption Trends Study | April 2018,” no. April, pp. 1–40, 2018.
- [75] BDO United State, “2018 BDO Cyber Governance Survey | See Results,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.bdo.com/insights/assurance/corporate-governance/2018-bdo-cyber-governance-survey-board-perspecti>
- [76] PR Newswire, "Cybersecurity Market Worth Over \$300bn by 2024: Global Market Insights, Inc." [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.prnewswire.com/news-releases/cybersecurity-market-worth-over-300bn-by-2024-global-market-isights-inc-863930577.html>
- [77] The SSL Store, “2018 Cybercrime Statistics: A closer look at the "Web of Profit",” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.thesslstore.com/blog/2018-cybercrime-statistics/>[82] HIMSS North America, “2016 HIMSS Cybersecurity Survey,” Himss, 2016. [Online]. Available: <http://www.himss.org/library/2016-himss-cybersecurity-survey>
- [78] N. Teodoro, L. Gonçalves, and C. Serrão, “Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements,” in 2015 IEEE Trust-com/BigDataSE/ISPA, vol. 1. IEEE, 2015, pp. 418–425.
- [79] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. Campbell, and M. N. Bashir, “It security and privacy standards in comparison: Improving fedramp authorization for cloud service providers,” in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE, 2017, pp. 1090–1099.
- [80] B. Duncan and M. Whittington, “Compliance with standards, assurance and audit: does this equal security?” in Proceedings of the 7th International Conference on Security of Information and Networks. ACM, 2014, p. 77.
- [81] K. Piromsopa, T. Klima, and L. Pavlik, “Designing model for calculating the amount of cyber risk insurance,” in 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). IEEE, 2017, pp. 196–200.
- [82] C. Pardo, F. J. Pino, F. García, M. Piattini, and M. T. Baldassarre, “An ontology for the harmonization of multiple standards and models,” Computer Standards & Interfaces, vol. 34, no. 1, pp. 48–59, 2012.

- [83] COBIT, “Control Objectives for Information and related Technology,” [Accessed: 31-Dec-2019]. [Online]. Available: <http://www.isaca.org>
- [84] C. Pardo, F. J. Pino, F. García, M. P. Velthius, and M. T. Baldassarre, “Trends in harmonization of multiple reference models,” in *International Conference on Evaluation of Novel Approaches to Software Engineering*. Springer, 2010, pp. 61–73.
- [85] D. Mellado, E. Fernández-Medina, and M. Piattini, “A common criteria based security requirements engineering process for the development of secure information systems,” *Computer standards & interfaces*, vol. 29, no. 2, pp. 244–253, 2007.
- [86] S.-H. Li, D. C. Yen, S.-C. Chen, P. S. Chen, W.-H. Lu, and C.-C. Cho, “Effects of virtualization on information security,” *Computer standards & interfaces*, vol. 42, pp. 1–8, 2015.
- [87] M. N. Alsaleh, G. Husari, and E. Al-Shaer, “Optimizing the roi of cyber risk mitigation,” in *2016 12th International Conference on Network and Service Management (CNSM)*. IEEE, 2016, pp. 223–227.
- [88] S. J. Shackelford, A. A. Proia, B. Martell, and A. N. Craig, “Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices,” *Tex. Int’l LJ*, vol. 50, p. 305, 2015.
- [89] T. Sommestad, G. N. Ericsson, and J. Nordlander, “Scada system cyber security—a comparison of standards,” in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–8.
- [90] M. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, “Technical security metrics model in compliance with iso/iec 27001 standard,” *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 4, pp. 280–288, 2012.
- [96] M. Saad Saleh, A. Alrabiah, and S. Haj Bakry, “A stope model for the investigation of compliance with iso 17799-2005,” *Information Management & Computer Security*, vol. 15, no. 4, pp. 283–294, 2007.
- [91] S. Almuhammadi and M. Alsaleh, “Information security maturity model for nist cyber security framework,” *Computer Science & Information Technology*, vol. 51, 2017.
- [92] L. Cyra and J. Gorski, “Scf—a framework supporting achieving and assessing conformity with standards,” *Computer Standards & Interfaces*, vol. 33, no. 1, pp. 80–95, 2011.
- [93] M. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, “Technical security metrics model in compliance with iso/iec 27001 standard,” *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 4, pp. 280–288, 2012.
- [94] National Institute of Standards and Technology, “National Institute of Standards and Technology | NIST,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.nist.gov/>
- [95] “Federal Information Processing Standards Publications (FIPS PUBS) | NIST,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.nist.gov/topics/federal-information-standards-fips>
- [96] International Organization for Standardization, “ISO - International Organization for Standardization,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.iso.org/home.html>
- [97] International, Electrotechnical, and Commission, “Welcome to the IEC - International Electrotechnical Commission,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.iec.ch/>
- [98] E. Humphreys, *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech House, 2016.

- [99] Common Criteria, “Common Criteria : New CC Portal,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.commoncriteriaportal.org/>
- [100] Acuity, “Store | Acuity Risk Management,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://acuityrm.com/store/Personal-Editions>
- [101] Vigilant Software, “VsRisk,” [Accessed: <https://www.vigilantsoftware.co.uk/topic/free-trial> 31-Dec-2019]. [Online].
- [102] Microsoft, “Download Microsoft Baseline Security Analyzer 2.1.1 (for IT Professionals) from Official Microsoft Download Center,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.microsoft.com/en-pk/download/details.aspx?id=19892>
- [103] “Download Microsoft Security Assessment Tool 4.0 from Official Microsoft Download Center,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://systemscenter.ru/scm.en/>
- [104] Belarc, “Products: Belarc Advisor,” [Accessed: [https://www.belarc.com/products\\_belarc\\_advisor](https://www.belarc.com/products_belarc_advisor) 31-Dec-2019]. [Online].
- [105] Michael Boelen, “GitHub - CISOfy/lynis: Lynis - Security auditing tool for Linux, macOS, and UNIX-based systems. Assists with compliance testing (HIPAA/ISO27001/PCI DSS) and system hardening. Agentless, and installation optional.” [Accessed: 31-Dec-2019]. [Online]. Available: <https://github.com/CISOfy/lynis>
- [106] Open SCAP, “Download | OpenSCAP portal,” [Accessed: 31-Dec-2019]. [Online]. Available: <http://www.open-scap.org/download/>[113] Javier Fernández-Sanguino, “Tiger - The UNIX Security audit and intrusion detection tool,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://www.nongnu.org/tiger/index.html#download>
- [107] Center for Internet Security, “CIS Configuration Assessment Tool CIS-CAT,” [Accessed: 31-Dec-2019]. [Online]. Available: <https://learn.cisecurity.org/cis-cat-lite>
- [108] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “Nist cloud computing reference architecture,” NIST special publication, vol. 500, no. 2011, pp. 1–28, 2011.
- [109] D. Dolezilek and L. Hussey, “Requirements or recommendations? sorting out nerc cip, nist, and doe cybersecurity,” in 2011 64th Annual Conference for Protective Relay Engineers. IEEE, 2011, pp. 328–333.
- [110] L. Shen, “The nist cybersecurity framework: Overview and potential impacts,” *Scitech Lawyer*, vol.10, no. 4, p. 16, 2014.
- [111] D. S. Herrmann, *Using the Common Criteria for IT security evaluation*. Auerbach Publications, 2002.
- [112] R. Kruger and J. H. Eloff, “A common criteria framework for the evaluation of information technology systems security,” in *Information Security in Research and Business*. Springer, 1997, pp. 197–209.
- [113] M. Brodin, “Combining isms with strategic management: the case of byod,” in 8th IADIS International Conference on Information Systems 2015, 14–16 March, Madeira, Portugal. IADIS Press, 2015, pp. 161–168.
- [114] E. D. G. Collard, S. Ducroquet and G. Talens, “A definition of information security classification in cybersecurity context,” *Proc. - Int. Conf. Res. Challenges Inf. Sci.*, vol. vol. 65, no. 3, p. 77–82, 2017.
- [115] T. Caddy, “Fips 140-2,” *Encyclopedia of Cryptography and Security*, pp. 468–471, 2011.

- [116] F. Ferdiansyah, "Analisis aktivitas dan pola jaringan terhadap eternal blue dan wannacry ransomware," JUSIFO (Jurnal Sistem Informasi), vol. 2, no. 1, pp. 44–59, 2018.
- [117] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49–51, 2011.