NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB), CABINET DIVISION

PAKISTAN SECURITY STANDARD FOR CRYPTOGRAPHIC & INFORMATION TECHNOLOGY SECURITY DEVICES

IT Security Guide Book

(Public Domain)

PAKISTAN STANDARDS AND QUALITY CONTROL AUTHORITY (PSQCA)
Standards Development Centre, PSQCA Complex, Gulistan-e-Jauher, Karachi

ICS: 35.020;35.030

PAKISTAN SECURITY STANDARD FOR CRYPTOGRAPHIC & INFORMATION TECHNOLOGY SECURITY DEVICES

IT Security Guide Book

(Public Domain)

DOCUMENT CODE INDEX	**:**	**PSS-GB-ITSEC-V1.0**
DOCUMENT TYPE	**:**	**PUBLIC**
CLASSIFICATION	**:**	**PUBLIC**
DATE OF ISSUE	**:**	**14 JUNE 2023**
ISSUING AUTHORITY	**:**	**PSQCA (PS: 5543-2021 -** ICS: 35.020;35.030**)**

PAKISTAN STANDARDS AND QUALITY CONTROL AUTHORITY (PSQCA)
Standards Development Centre, PSQCA Complex, Gulistan-e-Jauher, Karachi

Pakistan Security Standard for Cryptographic & IT Security Devices

Announcing the Standard for

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC & IT SECURITY DEVICES

This Pakistan Security Standard was adopted by the Pakistan Standards & Quality Control Authority Standards Development Centre on recommendation of National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, on 09-11-2021 after draft finalization and approval by National Standards Committee (NSC) for Information Technology. In the preparation of this standard the views of Cyber Security Specialists, Experts from Academia, Product Developers, Product Vendors, Testing Authorities, Regulatory Authorities and User Organizations have been taken into consideration.

1. Name of Standard. This standard may be called the **'**Pakistan Security Standard (PSS) for Cryptographic & IT Security (ITSec) Devices'. This standard consists of PSS-GB-CRYPTOSEC and PSS-GB-ITSEC.

2. Category of Standard. Information Security**,** Cryptography, Computer Security, IT Security, Network Security, Application Security, Cyber Security.

3. Explanation. PSS Guidebooks delineate guidelines for ensuring mandatory security and technical requirements that shall be satisfied by Cryptographic & ITSec Equipment (CE) and Cryptographic Algorithms or Primitives (CP) for sectors requiring such security systems to protect sensitive information in computer, telecommunication or cyber systems. The standard provides four increasing, qualitative levels of overall security; Level 1 (Low), Level 2 (Basic), Level 3 (Medium), and Level 4 (High); for the equipment comprising CE, CP and Supported Systems i.e. Key Management System and Network Management System; referred to as Crypto Equipment & Primitives (CEP) throughout PSS. These levels are intended to cover wide range of potential applications and environments in which a CE, CP or CEP may be employed.

PSS ITSec Guidebook outline guidelines for ensuring mandatory security and technical requirements that shall be satisfied by ITSec products and services. Till such time that a separate 'National IT Security Certification Scheme' is developed in line with Common Criteria (CC) Evaluation Methodology and promulgated, PSS will also serve as ITSec evaluation standard.

Vendors, developers and sponsors of Cryptographic & ITSec products shall request product or services evaluation from NTISB which will assign responsibility to any accredited laboratory for evaluation of Cryptographic & ITSec products. Pakistan National Accreditation Council (PNAC)

accredited Cryptographic & ITSec testing laboratories shall perform CEP compliance/conformance testing after receiving vendors/sponsors requests through NTISB. This standard supersedes TM-27, *Procedure for Introduction of a New Crypto Machine and Speech Secrecy Equipment in Pakistan*, in its entirety.

4. Approving Authority. Government of Pakistan.

5. Maintaining Agency. National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Government of Pakistan.

6. Applicability. Consumer electronics or IT systems or solutions that do not claim the provision of security functionality are excluded from PSS certification**.** List of items covered under PSS is as below:-

a. **Cryptographic**. Such articles that claim provision of confidentiality, integrity, authentication, availability and/or non-repudiation to users, networks or systems such as all kinds of cryptographic encryptors, hardware security modules, key generation, management or distribution systems, cryptographic tokens or systems for secure access or user authentication, cryptographic algorithms or protocols or operations, cryptography based communication or web applications, secure Virtual Private Networks or other such solutions.
b. **IT Security**. Such articles that claim provision of specific cyber security functions such as all kinds of firewalls, network routers, high capacity switch, intrusion detection & prevention, endpoint security, secure access control systems, security information management, security information and event management, secure operating systems, secure applications, secure database management, anti-denial of service, anti-virus, anti-spyware, anti-theft, anti-malware or any other such solution.

7. Applications. NTISB shall validate Cryptographic & ITSec equipment to PSS. Products validated as conforming to PSS shall be accepted and preferred by the government organizations and departments for protection of sensitive information till such time that PSS becomes mandatory. The goal of PSS is to promote use of validated Cryptographic & ITSec products and services and provide critical sectors with a security metric to use in such procurements. This standard **shall also** be used in designing and implementing cryptographic and ITSec products and services that government organizations and critical sectors either operate or are operated for them. After analyzing guidebooks, vendors and developers of security solutions will request NTISB for provision of restricted release documents that contain additional information. The adoption and use of this standard is also encouraged for private and commercial sector organizations. Cryptography-based security systems may be utilized in various computer, telecommunication, and cyber security

applications (e.g., authentication, authorization, access control, data at rest and motion, personal identification, IP networks and fixed telecom network communications, wireless communication i.e. radio, mobile, satellite etc.) that may be used in various operating environments (e.g., centralized or distributed environments, remote access scenarios and hostile environments etc.). The cryptographic functions for data secrecy, data integrity, personal identification, digital signatures and management of cryptographic keys etc. are based on factors that are specific to the application and operating environment. Users of critical sectors shall select equipment or services of a level of security appropriate for the organizational requirements commensurating to application and environment in which the equipment or service will be utilized or provided. Developers of local industry will acquire PSS guidance from NTISB for designing security equipment and services for local as well as export markets. Vendors or sponsors of security equipment will approach NTISB for conduct of security strength testing through Evaluation Labs that will assure users regarding achieved security level against vendor or developer claims.

8. Interpretation. Questions concerning the content and specifications of this standard shall be addressed to: Secretary, NTISB, Cabinet Division, Islamabad (www.cabinet.gov.pk).

9. Qualifications. The security requirements specified in this standard are approved by Pakistan Standards and Quality Control Authority (PSQCA) which are based upon information provided by various sectors such as Public, Private, Academia, Industry and International Standards from NIST, ISO/IEC and Common Criteria etc. The requirements are designed to aid in protecting sensitive data and services against attacks by adversarial entities e.g. insiders, hackers, hacktivists, unauthorized entities, economic and non-aligned competitors etc. While the security requirements specified in this standard are intended to maintain the security provided by a Cryptographic & ITSec product, conformance to this standard is not sufficient to ensure that a particular product is secure. User of a Cryptographic & ITSec product is responsible for its secure configuration, operation, maintenance and ensuring that the security provided by a product is sufficient and acceptable to the owner of the information that is being protected. Any residual risk is acknowledged and accepted by the responsible authority in each organization along with the enforcement responsibility of NTISB recommendations. New or revised requirements may be needed to meet technological and economic changes with scientific and cryptographic evolution. This standard shall be reviewed, revised and updated after every 3 years or as and when required on the instructions of NTISB who will designate a Review Committee from stakeholders**.** PSS will retain relevance in implementation of information, IT and cyber security aspects of national policies on use of cyber, cloud, broadband, data protection and other such policies as and when these are promulgated. All users will obtain latest version from PSQCA, NTISB and provide required information and data in accordance with the provisions of

latest PSS publications. For guidance on subjects not covered by PSS, respective standard/guideline/best practice of US NIST, Common Criteria, OWASP, SANS, ISO/IEC, ILAC etc. may be referred.

10. Implementation Schedule. This standard will become mandatory in 5x years' time frame (with effect from **1st June 2028**). However, its earlier adoption is recommended and sectors requiring immediate adoption for deployment may undertake appropriate actions at their level with consultation of respective regulators and/or PPRA. As PSS security requirements are in line with International security standards, relevant product certifications such as US NIST FIPS 140-2 and/or Common Criteria etc. may be produced by vendors and accepted till such time that PSS certification becomes mandatory for critical sectors. NTISB shall devise business model and strategic plan to facilitate and encourage establishment of Cryptographic & ITSec Evaluation labs for PSS based testing in public, private and academia sectors. Till such time (which shall not exceed 2 years) that labs get accreditation under National Accreditation Standard for Crypto & ITSec Evaluation Labs (NASCEL), decision for employing existing infrastructure and facilities in public sector rests with NTISB. Before the standard becomes mandatory, sectors requiring security of information & systems shall develop phase-out and procurement plans to comply with PSS requirements. NTISB shall maintain validated product list on NTISB website and devise a controlled mechanism for Vendors and Developers for restricted release of additional technical documents depending upon type, configuration and operational environment of the security solution. Organizations may purchase any of the products on the NTISB validated product list as per their environment, operational and information security requirements. Use of such equipment will however be subject to conformance to the security requirements, applicability of the security profile of the equipment or service and NTISB guidance.

Sr No	**Sector**	**Timelines**		
		PSS Compliance (Product Conformance to PSS)		**PSS Certification** (Product Evaluation as per PSS)
		New Procurement	Existing Operational Products	
a	**Government** (Federal, Provincial, Ministries, Regulatory Bodies, Education, Health, LEAs, Energy Sector, Railways, Critical Organizations such as CAA, NADRA, Immigration, Ehsaas, etc.)	• International Certifications (FIPS, CC, etc.) may be acceptable as per sector regulator / user organization security requirement till PSS	• Phase-Out Plan to be developed before PSS becomes mandatory. • Product Phase out may be implemented as per sensitivity of	Mandatory after **5x years**

Sr No	Sector	Timelines		
		PSS Compliance (Product Conformance to PSS)		PSS Certification (Product Evaluation as per PSS)
		New Procurement	Existing Operational Products	
b	**Defense** (Services including all related organizations)	becomes mandatory or as per priority set by respective sector regulator. • Must be PSS Compliant after **5x years**. • Interoperability with existing systems to be ensured.	organization and information alongwith financial implications.	
c	Semi-Government or Autonomous bodies			
d	**Telecom & ISPs** (including mobile, data and fixed telephony service providers)			
e	**Banking and Financial**			
f	**Private & Industrial Sectors**		If dealing with **Personal Identifiable Information (PII), Intellectual Property (IP)**, **sensitive projects**, **sensitive data** or **related** to **critical infra** etc, Phase-Out Plan to be developed before PSS becomes mandatory after **5x years** or as per respective sector regulator priority.	

Table - PSS Implementation Schedule

11. Where to obtain copies of this Standard. This publication is available at NTISB and PSQCA websites. Other computer security publications issued by NTISB are also available at NTISB website.

12. List of Authors, Contributors, Reviewers & Approval Committees

S/N	Name	Information	
PSS AUTHORS PANEL			
1.	Dr Nassar Ikram	dr_nassar_ikram@yahoo.com	National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Pakistan +92-051-9208054 +92-051-9207930 pss-devpanel@cabinet.gov.pk
2.	Dr Nadeem Sial	nadeem@commoncriteria.gov.pk	
3.	Kashif Rahim	kashif@commoncriteria.gov.pk	
4.	Dr Asad Khan Sadozai	mabu.maaz@gmail.com	
5.	Muhammad Umair Tariq	m.omair.tarik@gmail.com	
6.	Uroosa Kiran	uroosakiran@gmail.com	
7.	Muhammad Amir	muhammad.aamir.tariq@gmail.com	
8.	Ali Afzal Awan	aaa.phdis@students.mcs.edu.pk	
9.	Raja Zeeshan Haider	rhaider.phdismcs@student.nust.edu.pk	
PSS REVIEWING PANEL			
1.	Mansoor Sehgal	Secretary, NTISB	
2.	Dr Baber Aslam	ababer@mcs.edu.pk	
3.	Syed Junaid Imam	Member IT, MoIT&T	
4.	Dr Muhmmad Tayyab Ali	MCS, NUST, Islamabad	
5.	Sharjeel Zareen		

S/N	Name	Information	
6.	Dr Liaqat Ali Khan	Air University, Islamabad	
7.	Dr Muhammad Qasim Saeed		
8.	Khalid Habib	Bahria University, Islamabad	
9.	Dr Mureed Hussain	National Engineering & Scientific Commission (NESCOM)	
10.	Dr Sheraz Ahmed		
11.	Dr Safdar Shaheen		
12.	Dr Mehreen Afzal	Director Security & GRC, pkCERT, MoIT&T	
13.	Abdul Rehan Khan	Department of Communication Security (DCS)	
14.	Ghazenfer Abbas	Pakistan Telecommunication Authority (PTA)	
15.	Dr Maajid Khan	Institute of Space Technologies (IST), Islamabad	
16.	Mohsin Ali	Inbox Business Tech (Pvt) Ltd	
17.	Mahir Mohsin Sheikh	Trillium Information Security Systems	
18.	Ismat Gul Khattak	Director General, Pakistan National Accreditation Council (PNAC)	
19.	Azhar Khan	Director, Pakistan National Accreditation Council (PNAC)	
PSS STAKEHOLDERS PANEL			
1.	Shazia Shah	National Telecom Corporation (NTC)	
2.	Irfan Rafi		
3.	Faisal Ayub	National Database and Registration Authority (NADRA)	
4.	Muhammad Sibtain	Department of Communication Security (DCS)	
5.	Aalishan Akhter	Ministry of Information Technology and Telecommunication (MoIT&T)	
6.	Muhammad Imran	Frequency Allocation Board (FAB)	
7.	Muhammad Ilyas	Ministry of Interior (MoI)	
8.	Zafar Mehboob		
9.	Dr Saeed ur Rehman	Pakistan Standards and Quality Control Authority (PSQCA)	
10.	Dr Muhammad Wasif Nisar		
11.	Abdul Ghaffar Niazi		
12.	Wahab Feroze	Ministry of Science and Technology (MoST)	
13.	Dr Shoukat Ali	Pakistan Software Export Board (PSEB)	
14.	Imran Nazir	National Information Technology Board (NITB)	
15.	Usman Ghani	Ministry of Industries Pakistan (MoIP)	
16.	Abid Hussain Kalwar		
17.	Ali Murtaza	State Bank of Pakistan (SBP)	
18.	Faisal Anwar	United Bank Limited (UBL)	
19.	Waqas Mehmood	Higher Education Commission (HEC)	
PSQCA APPROVING PANEL			
1.	Meritorious Prof Dr S.M. Aqil Burney	Chairman	Head of Actuarial Science and Risk Management (IOBM), UoK, Karachi
2.	Muhammad Asif Riaz	Vice Chairman	ENSTA Tech Digital Array, Private Limited, Karachi,
PSQCA APPROVING PANEL MEMBERS			
1.	Dr Syed Irfan Nabi	Assistant Professor, Institute of Business Administration (IBA) , Karachi	
2.	Iqbal Ahmad Jamal	Chairman (ICT-TC1), PIBAS Pakistan, Pvt Limited	
3.	Ishfaque Ahmed Khanzada	Chairman (ICT-TC6), Head of ICT Infra & Network, University of Karachi	
4.	Asif Rafiq	Senior Lecturer, DHA Suffa University, Karachi	
5.	Tariq Umer	Chairman (ICT-TC3), Assistant Professor COMSATS University, Lahore	
6.	Dr Humera Tariq	Chairman (ICT-TC5), Associate Professor, University of Karachi	
7.	Rana Shahzad Qasir	Chairman (ICT-TC5), Cyber Crime, Federal Investigation Agency (FIA) Karachi	
8.	Muhammad Tayyab Chaudhry	Chairman (ICT-TC7), Assistant Professor, COMSATS University, Lahore	
9.	Dr Abdul Razzaque	Chairman (ICT-TC7) Associate Professor, MCS, NUST	
10.	Dr. Muhammad Akram Iftikhar	Chairman (ICT-TC-2) Assistant Professor, COMSATS University	
11.	Imran Nazir	Assistant Secretary, NTISB	
12.	Kamran Rasheed	Deputy Secretary, NTISB	
13.	Kashif Rahim	Director, NTISB	
14.	Muhammad Umair Tariq	Director Technical Development Centre, pkCERT, MoIT&T	
15.	Uroosa Kiran	Deputy Director, NTISB	
16.	Anjum Parveen	Deputy Director (IT & ICT), Secretary to the Committee NSC/TC , Standards Development Centre, PSQCA , Karachi	

Table - PSS Authors, Reviewing & Approving Panels

FOREWORD

1. This Pakistan Standard was adopted by the authority of the Board of Directors for Pakistan Standards and Quality Control Authority after approval by the Technical Committee for "Information technology - Information Security, Cyber Security and Privacy protection ICT-TC3" had been approved and endorsed by the IT & ICT National Standards Committee on 09-11-2021.
2. This Pakistan Standard is formulated based on information provided by varied sectors such as public, private, academia, industry and International Standards from NIST, ISO/IEC and Common Criteria etc. Standard named it as "Pakistan Security Standard for Cryptographic & ITSec Devices- PSS Guide Book" and "Pakistan Security Standard for Cryptographic & ITSec Devices- ITSec Guide Book". As per technical committee it was deemed suitable to adopt it.
3. This Pakistan Standard is formulated based on information provided by varied sectors such as public, private, academia, industry and International Standards from NIST, ISO/IEC and Common Criteria etc. "Pakistan Security Standard for Cryptographic & ITSec Devices" and its use hereby acknowledged with thanks.
4. This standard is subject to periodical review in order to keep pace with the development in industry. Any suggestions for improvement shall be recorded and placed before the revising committee in due course.
5. This standard is intended chiefly to cover the technical provisions relating to this standard and it does not include all the necessary provisions of a Contract.
6. Scheme Publication PSS-GB-CRYPTOSec and PSS-GB-ITSec provides insight into PSS and procedural guidelines for Vendors, Developers and Sponsors (VDS) on evaluation, development and validation of COMSEC products. It will also help standardize indigenous development of information security (INFOSEC) products, components, services and procedures in Pakistan in line with modern trends. Also, will prepare and facilitate understanding of responsibilities during design and development stages as well as before conduct of evaluation, during the evaluation process and subsequent formalities for culmination of evaluation process.

In the event of any questions concerning this publication or for further information, please consult NTISB at given address.	
Address	Secretary, National Telecommunication and Information Technology Security Board (NTISB), Cabinet Division, Pakistan
Telephone	+92-051-9208054; FAX +92-051-9207930
Email	pss@cabinet.gov.pk; pss@ntisb.gov.pk

AMENDMENT RECORD

Amendments to this document will be published as and when required.

Date	Version	Details of Affected Sections

ABBREVIATIONS

ACK	Acknowledge
API	Application Programming Interface
AS	Assertion
AVL	Accredited and Validated Lab
BC	Block Cipher
CA	Certification Authority
CC	Common Criteria (for Information Technology Security Evaluation)
CCRA	Common Criteria Recognition Agreement
CE	Cryptographic Equipment
CEVaL	Cryptographic Evaluation & Validation Lab
CEP	Cryptographic Equipment and Cryptographic Primitives
COMSEC	Communication Security
CP	Cryptographic Primitives
DDOS	Distributed Denial Of Service
DNS	Domain Name Server
DOS	Denial Of Service
DTR	Derived Test Requirements
EAAPP	Evaluation Application, Acceptance and Preparation Process
ECAC	Electronic Certification Accreditation Council
EL	Evaluation Lab
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENISA	European Network and Information Security Agency
ESM	Evaluation Startup Meeting
ETL	EMI/EMC/Environmental Testing Laboratory
EVP	Evaluation and Validation Process
EWP	Evaluation Work Plan
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FTP	File Transfer Protocol
GPS	Global Positioning System
GR	General Requirements
HTTP	Hypertext transfer Protocol
ICMP	Internet Control Messaging Protocol
ICT	Information Communication Technology
IDS	Intrusion Detection System
IM	Instant Messaging
INFOSEC	Information Security
IOS	IPhone Operating System
IP	Internet Protocol

IPC	Interrupt Procedure Calls
IPS	Intrusion Prevention System
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
IVR	Implementation Verification Requirements
MITM	Man In The Middle
NDA	Non-Disclosure Agreement
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NTISB	National Telecommunication and Information Technology Security Board
NVLAP	National Voluntary Lab Accreditation Procedure (US FIPS NVLAP)
OS	Operating System
OSI	Open System Interconnection
PC	Personal Computer
PII	Personal Identifiable Information
PNDA	PSS Non-Disclosure Agreement
PSS	Pakistan Security Standard for Cryptographic & ITSec Devices
RF	Radio Frequency
SDI	Secure Design and Implementation
SDM	Scope Defining Meeting
SNIA	Storage Networking Industry Association
SSER(SP)	Security Strength Evaluation Report (SP) by NTISB-PSSIS to Sponsor
SSL	Secure Socket Layer
SYN	Synchronization
TLS	Transport Layer Security
TOE	Target Of Evaluation
UI	User Interface
UDP	User Datagram Protocol
VDS	Vendor/Developer/Sponsor
VWP	Validation Work Plan

REFERENCES

Following standards/guidelines were studied prior drafting this document. Some of the contents or ideas have been developed and reproduced from below documents.

1. International Common Criteria (CC) for ITSec Evaluation
2. Common Criteria Firewall Protection Profile V2.0
3. Common Criteria Protection Profile for Network Devices
4. Protection Profile for Application Level Firewall in High Robustness Environments
5. ICSA labs Firewall Certification Criteria, Baseline Module – Version 4.1x
6. Guidelines on Firewalls and Firewall Policy – NIST Special Publication 800-41
7. ISO-27001 – Information Security Management
8. Open Web Application Security Project (OWASP) – OWASP Mobile Application Security Verification Standard v0.9.2
9. Technical Guide to Information Security Assessment and Testing – NIST Special Publication 800-115
10. Storage Networking Industry Association (SNIA) – Storage Security Best Current Practices Version 2.1.0
11. European Network and Information Security Agency (ENISA) – Smartphone Secure Development Guidelines for App Developers
12. Guidelines on Security and Privacy in Public Cloud Computing – NIST SP 800-144
13. CSA Security Guidance For Critical Areas of focus in Cloud Computing v3.0
14. ISO/IEC TS 27110:2021 Information Technology, Cybersecurity and Privacy Protection – Cybersecurity Framework Development Guidelines
15. CryptoCurrency Certification Consortium (C4)
16. Blockchain Networks: Token Design and Management Overview – NIST IR-8301
17. Guidelines on Firewalls and Firewall Policy – NIST Special Publication 800-41
18. Resilient Inter Domain Traffic Exchange: BGP Security and DDoS Mitigation – NIST Special Publication 800-189
19. Guide to Intrusion Detection and Prevention Systems (IDPS) – NIST Special Publication 800-94
20. Security Guidelines for Storage Infrastructure – NIST Special Publication 800-209
21. Foundational Cybersecurity Activities for IoT Device Manufacturers – NISTIR 8259
22. Evaluation of Cloud Computing Services Based on NIST SP 800-145 – NIST Special Publication 500-322
23. Outsourcing to Cloud Service Providers (CSPs) By State Bank of Pakistan – BPRD Circular No. 04 of 2020
24. Guide to Industrial Control Systems (ICS) Security – NIST Special Publication 800-82
25. Good Practice Guide Process Control And SCADA Security – Centre for the Protection of National Infrastructure

GLOSSARY OF TERMS

Access Control

Restricts access of resources only to the privileged entities.

Accountability

A property that ensures that the actions of an entity may be traced uniquely to that entity.

Approved

An algorithm / function or scheme that is evaluated as per PSS and passes the required testing / analysis.

Audit Logs

An audit log, also called an audit trail, is essentially a record of events and changes. IT devices across your network create logs based on events. Audit logs are records of these event logs, typically regarding a sequence of activities or a specific activity.

Authentication

Authentication is a process of establishing the origin of information or determines an entity's identity.

Authorization

Access privileges that are granted to an entity are called authorization.

Availability

Timely, reliable access to information by authorized entities.

Certificate

A set of data that uniquely identifies an entity, contains the entity's public key and other information and is digitally signed by a trusted party, thereby binding the public key to the entity.

Certification Authority

The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates and ensuring compliance to a PKI policy.

Compromise

The unauthorized disclosure, modification, substitution or use of sensitive data.

Confidentiality

The property that sensitive information is not disclosed to unauthorized entities.

Contingency Planning

A plan that is made for dealing with an emergency, or with something that might possibly happen and cause problems in the future.

Cyclomatic Complexity

Cyclomatic complexity of a code section is the quantitative measure of the number of linearly independent paths in it. It is a software metric used to indicate the complexity of a program.

Fuzzing

Fuzz testing (fuzzing) is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks. It involves inputting massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash.

Integrity

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner is called integrity.

Network Storage System

It is a storage device connected to a network that allows storage and retrieval of data from a centralized location for authorized network users and heterogeneous clients.

Next Generation Firewalls (NGFWs)

A next-generation firewall is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection, an intrusion prevention system.

Peer-to-peer Attacks

Peer-to-Peer attacks exploit the fabric of peering technology to perform attacks. These attacks distinguish themselves from other types of attacks because of the following:-

1) Attacker doesn't have to communicate with the clients for subversion and
2) the automated nature of Peer-to-Peer technology can allow for BOT like amplification of an attack with the permission of the victim.

Penetration Testing

Penetration testing is a simulated cyber-attack where professional ethical hackers break into corporate networks to find weaknesses.

Security Policy

Information security policies are usually the result of risk assessments, in which vulnerabilities are identified and safeguards are chosen. Each policy will address a specific risk and define the steps that must be taken to mitigate it.

Smurf

The Smurf attack is a distributed Denial-Of-Service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

Stateful Inspection Firewalls

A stateful firewall is a network-based firewall that individually tracks sessions of network connections traversing it.

Teardrop

A teardrop attack is a Denial-Of-Service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

Volume based Attacks

Volume-based attacks are characterized by an excessive amount of traffic (sometimes in excess of 100 Gbps). They do not mandate large amounts of traffic to be generated by one location or one source. The attack’s goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

Vulnerability

A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

Zero-day

The term zero-day refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released.

DOCUMENT ORGANIZATION AND SCOPE

This document gives an insight into PSS and describes in detail roles of Vendor, Developer and Sponsor (VDS) in evaluation process of IT Security products and services. It consists of 8x chapters with supporting annexures. ***Chapter 1*** describes evaluation of ITSec equipment, cyber security framework and security levels of PSS. ***Chapter 2*** describes documentation and basic requirements. ***Chapter 3*** provides information related to Firewall, IDS/ IPS, smart devices and cloud based services. ***Chapter 4*** includes audit scope, audit process and screening processes. ***Chapter 5*** provides guidelines for security of PKI architecture and physical/ logical security requirements. ***Chapter 6*** provides information related to secure software applications, architecture, data storage & privacy, and code quality. ***Chapter 7*** provide guidance on blockchain and virtual currency based assets while ***Chapter 8*** deals with export of ITSec equipment.

Table of Contents

List of Figures

Chapter 1

Overview

1.1 Introduction

IT Security is concerned with the protection of information assets. Information and the systems that process it are among the most valuable assets of any organization. Assets are entities that an organization places value upon. Examples include:-

1) Access to a classified facility or information
2) Contents of a file or a server
3) Availability of an electronic process
4) Ability to use an IT system

Many assets are in the form of information that is stored, processed or transmitted by IT products to meet requirements laid down by authorized owners/handlers of that information. Information owners/handlers require confidentiality, availability and integrity of this information and its modification/dissemination should be strictly controlled. There must be sufficient IT Security Equipment in place for protection of such assets. This high-level relationship can be illustrated by the following figure:-

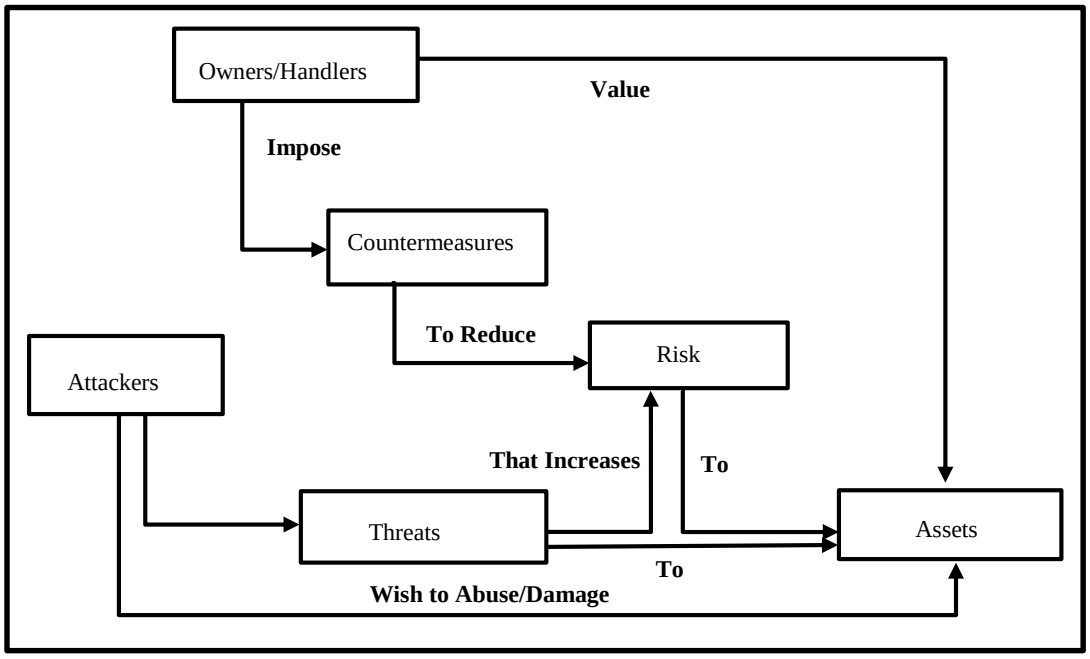

Figure 1.1: IT Security Relationships

Owners/handlers may lack the knowledge, expertise or resources necessary to judge the sufficiency or correctness of IT Security Equipment, and they should not rely solely on the statements of the developers of these equipment.

1.2 Evaluation of ITSec Equipment

ITSec equipment may be erroneously designed and implemented, and may therefore contain loopholes that lead to vulnerabilities. By exploiting these vulnerabilities, attackers may still damage and/or abuse the assets. Existence of these vulnerabilities may be result of:-

1) Accidental errors made during development
2) Bad design
3) Intentional addition of malicious code
4) Poor in-house testing

To analyze security implementation of ITSec equipment, an evaluation is required to increase the confidence in the sufficiency, correctness and security of the implemented countermeasures in such equipment.

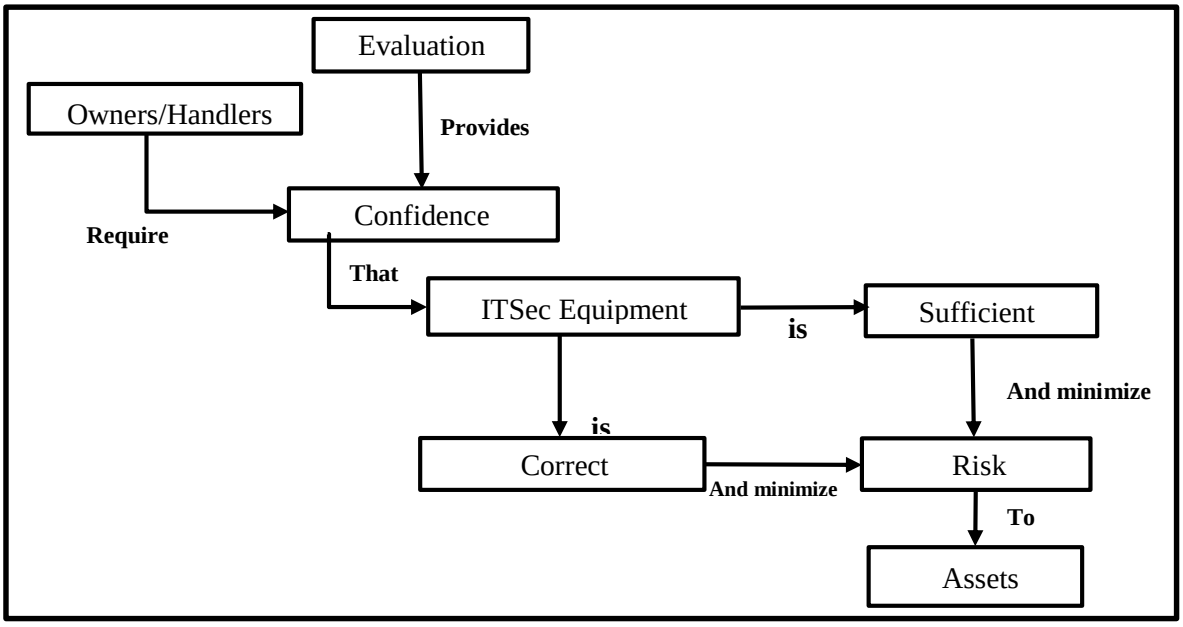

Figure 1.2: ITSec Evaluation Relationship

By providing an independent assessment of a product's ability to meet security requirements, this standard will give more confidence in the security of IT products to its users.

Due to their diverse nature, ITSec equipment evaluation cannot be confined to a controlled standard. Accordingly, instead of restricting procedures into a single DTR document, ITSec evaluation shall follow existing best practices and renowned international standards such as Common Criteria (CC), NIST, etc. Formulating ITSec evaluation procedures necessitates implementation of a comprehensive National Certification Scheme for ITSec products under

which all ITSec equipment will be evaluated and certified. Pakistan already holds membership as a certificate consumer at the Common Criteria Recognition Agreement (CCRA). To reap maximum benefits, the National Certification Scheme for ITSec evaluation will be formulated at par with other international schemes.

1.3 Categories of ITSec Equipment

This document is applicable to (but not limited to) evaluation of the following types of ITSec equipment:-

1) All kinds of Firewalls
2) Intrusion Detection and Prevention Systems (IDS/IPS)
3) DoS/DDoS Mitigation Systems
4) Network Storage Systems
5) Routers and Switches
6) Smart Device Security
7) Cloud Based Infrastructure
8) Endpoint Security Solutions
9) Access Control Systems
10) Security Information and Event Management
11) Secure Operating Systems, Applications, Database Management
12) Or any other such solution providing a Cyber Security Function

Note: ***IP encryptors, although fall under the category of ITSec, have been covered in the Cryptographic Equipment and SDI standards due to the underlying cryptographic nature of the device. However, if an IP encryptor contains additional features such as firewalling, etc., these shall be evaluated against related requirements laid out in ITSec standard. Similarly, if any ITSec equipment performs cryptographic or key management functions, these shall be evaluated as per relevant standards of PSS-GB-CRYPTOSEC.***

1.4 Cyber Security Framework

Cyber space has been weaponized with countries facing targeted cyber intrusion, ransomware, intellectual property theft, data exfiltration and service denial campaigns by hacktivists, script-kiddies, non-state actors and adversarial nations. Cyber threats are continually evolving and protection of data, privacy, users and organizations has become a constant challenge. Therefore, business groups, government agencies and organizations are encouraged to produce documents, devise protection methodologies, design and develop tools and organize security

frameworks to ensure cybersecurity of activities. With establishment of National Computer Emergency Response Team (pkCERT), holistic efforts will now be directed towards development of such cybersecurity tools, techniques and procedures.

Another divergent paradigm is harmonizing different conceptual frameworks to meet requirements of individuals and organizations. It is important that user community realizes importance of cybersecurity practices and raise cybersecurity departments within organizations to cater for cybersecurity imperative essentials. Therefore, to ensure that a minimum set of concepts are described, in line with ISO/IEC 27110-2021, this document also lists below minimum set of concepts which can be extended by addition and further elaboration of the concepts required for diverse nature of the user community:-

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

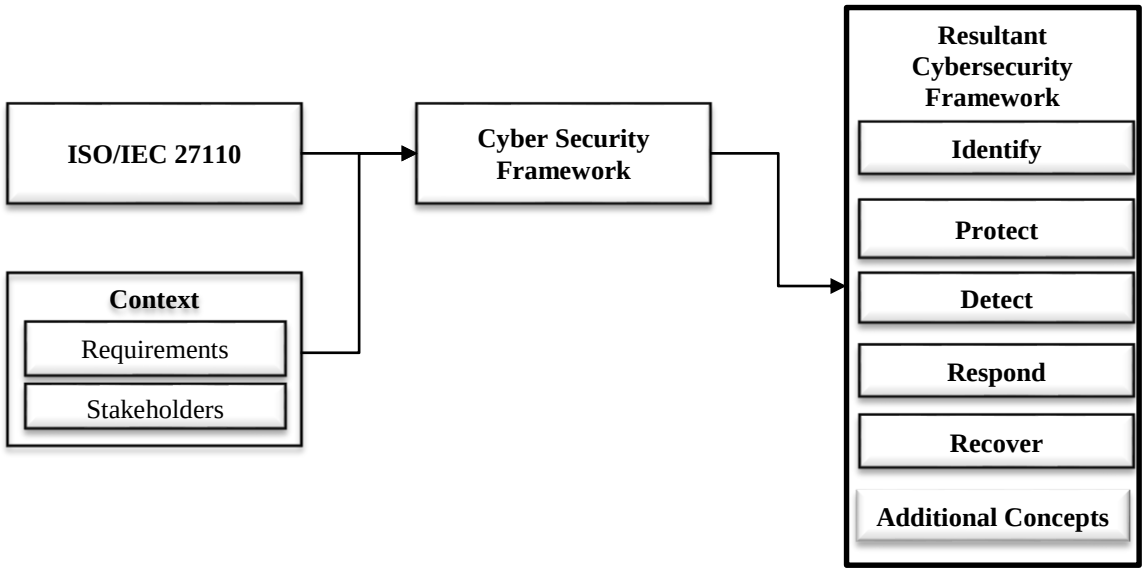

Figure 1.3: Cyber Security Framework ISO/IEC 27110:2021

1.5 Cyber Security for Industrial Control Systems (ICS)

Industrial Control System (ICS) is a general term that encompasses several types of control systems, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Cyber Physical Systems (CPS) and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors as well as critical infrastructures e.g., electricity, natural gas, gasoline, water, waste treatment, transportation etc.

ICS systems were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control systems are robust, while the security of these systems is often weak. This makes some ICS networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Action is required by all organizations, government or commercial, to secure their ICS network as part of the effort to adequately protect the nation's critical infrastructure. Security of ICS systems can be improved by adopting guidelines and recommendations mentioned in NIST Special Publication 800-82, Centre for the Protection of National Infrastructure (CPNI) and other similar best practices available in literature and announced by pkCERT, from time to time.

1.6 PSS Composition

Broadly, PSS can be divided into 2x main categories (Figure 1.4) i.e. PSS Implementation Scheme with 4x documents (2x Public Domain Documents and 2x Restricted Release Documents) and Security Standard with 10x documents. General Requirements (GR) define technical, operational, cryptographic requirements with Derived Test Requirement (DTR) documents further elaborating evaluation test requirements and facilitates understanding of VDS in enabling AVL to perform required testing and evaluation.

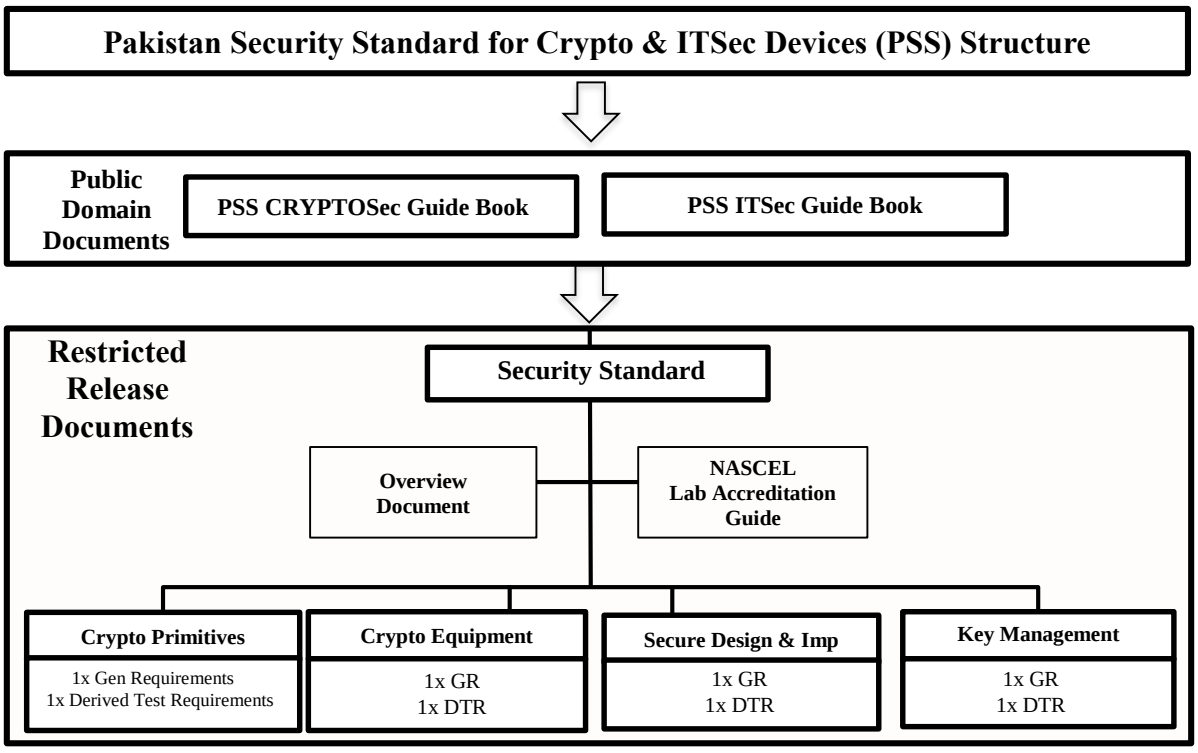

Figure 1.4: PSS Composition

1.6.1 PSS Implementation Scheme (PSSIS)

PSSIS is the framework designed for stipulating procedures, methodologies and functions of NTISB, ELs, VDS and lab accreditation mechanism. This framework consist of following:-

1) **PSS Cryptographic and ITSec Guide Books** provide an extensive insight into functions, roles, processes and methodologies established for evaluation of COMSEC and ITSec equipment, algorithms, protocols, services etc. The guide books will be for public release and used as reference when furnishing technical documentation for security evaluation or when designing and developing such security solutions. Due to their diverse nature, ITSec equipment evaluation cannot be confined to a controlled standard. Accordingly, instead of restricting procedures into a single DTR document, ITSec evaluation shall follow best practices and international standards till such time that National Certification Scheme on the lines of Common Criteria Recognition Agreement (CCRA) is developed.
2) **PSSIS-NASCEL Guide Book** for National Accreditation Standard for Crypto & ITSec Evaluation Labs is a restricted release document and defines mechanism, requirements and set of procedures for establishing and accrediting evaluation labs. Final accreditation will be granted by Pakistan National Accreditation Council (PNAC) following a successful completion of accreditation process which includes submission of an application, an on-site assessment by PNAC certified assessors, resolution of any non-conformity identified during on-site assessment, participation in proficiency testing and technical evaluation. This accreditation is only restricted and limited to government/ semi-government/ private organizations within Pakistan that carryout security strength evaluations.

1.6.2 Security Standard

Security Standard is restricted release which will be provided to VDS upon request depending upon type, configuration and operational environment of CEP:-

1) **Cryptographic Primitives Standard** sets forth requirements to evaluate crypto algorithms, protocols, formal verifications and security mechanisms.
2) **Cryptographic Equipment Standard** stipulates requirements to evaluate crypto equipment and its performance and functional testing.
3) **Secure Design and Implementation Standard** defines secure design and implementation techniques, guidelines and mechanisms.

4) **Key Management System Standard** defines criteria for key management life cycle.

1.7 Compliance and Certification Roadmap

PSS provides assurance of ITSec claims on any product or service containing information technology. In order to streamline alignment of desired ITSec in an earliest possible timeframe, there is a need to introduce a scheduled PSS implementation plan that can facilitate critical sectors, organizations and end users to align their existing as well as future ITSec infrastructure. Timelines for PSS compliance (i.e. conformance to PSS) and PSS certification (i.e. detailed evaluation as per PSS) of products and services are as per PSS Gazette Notification (***Annex A***).

Chapter 2

General Requirements for ITSec Equipment

2.1 Introduction

The widespread digitization of almost every sphere of daily life activities and necessities has resulted in increased dependence on IT systems. Critical organizations are also heavily dependent upon deployed IT infrastructure for provision of their critical services. Simultaneously, efforts for denial and compromise of these IT infrastructure have increased manifold. Ensuring defense in depth security of IT products and services is therefore a keystone requirement. To address the pressing need for safeguarding critical infrastructure, sensitive data, and public trust, a comprehensive framework for PSS has been crafted to define the general requirements for ITSec equipment. This chapter defines the general and basic requirements for the selection, deployment, and maintenance of ITSec equipment.

2.2 Documentation Requirements

1) A comprehensive security policy shall be formulated for each Target of Evaluation (TOE) employed in the network. The security policy shall delineate the security management structure and clearly assign security responsibilities, and lay the foundation to reliably measure security effectiveness and compliance of TOE. The policy shall be approved by key affected parties and shall cover security planning, risk management, review of security controls, rules of behavior, life-cycle management, processing authorizations, personnel, physical and environmental aspects, contingency planning, incident response, access controls and audit logs of TOE.
2) Procedures for implementing rules specified in the security policy shall be formally and completely documented in the form of technical and operational manuals. Documentation shall cover all major operations of the TOE, security controls, rules of behavior, processing authorizations, support and operations, physical and environmental aspects, incident response, access control and audit logs.
3) Documentation shall contain a formal process for approving and testing all network connections and changes to TOE configurations. This will help prevent security problems that might arise due to misconfiguration of the TOE and neighboring network devices in a network.

4) Documentation shall contain a detailed network diagram that identifies all connections between the TOE and other network devices, including wireless network devices.
5) Documentation shall contain a diagram showing information flows between the TOE and other network systems and sub-systems.
6) Documentation shall contain a description of groups, roles and responsibilities for management and configuration of TOE.
7) Documentation shall specify the operational environment of the TOE and list all assumptions, threats and vulnerabilities that exist for the TOE in that operational environment.
8) Documentation shall contain test methodology for testing the TOE against the listed threats and vulnerabilities.

2.3 Basic Requirements for ITSec Equipment

1) The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
2) The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.
3) The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information from a previous information flow is not transmitted in any way.
4) Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
5) The TOE must protect the confidentiality of its session with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network. The adopted encryption algorithm must fulfill General Requirements for Cryptographic Primitives (GR for CP).
6) The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
7) The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
8) The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

9) The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
10) The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized entity.
11) The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
12) If the TOE does not fulfill any of the requirements stated above, or uses other mechanisms to ensure security of TOE, vendor shall justify the use of the mechanism and prove that deviation from the above mentioned requirements does not impact the security functionality of the TOE.
13) For evaluation request, process and other modalities (timelines, payments etc.) refer to relevant chapters and annexures of PSS-GB-CRYPTOSEC.

Chapter 3

Network Security Devices

3.1 Introduction

Security of networked systems has given rise to multiple cyber threats, necessitating the establishment of robust standards and guidelines for network security. This chapter aligns with the PSS framework, addressing the specific requirements and best practices for network security devices, offering a comprehensive resource for practitioners, policy makers and industry professionals. The compliance of ITSec devices with PSS is an essential endeavor, ensuring that network security is not only effective but also cohesive and consistent across diverse organizations and critical infrastructure.

3.2 Firewalls

In addition to the General Requirements for ITSec equipment, Common Criteria and NIST Special Publication 800-41, following essential requirements shall also apply on firewalls:-

1) The firewall shall have the capability to log the following event types:-
    a) All permitted inbound access requests from public network clients on a private or internal network server.
    b) All permitted outbound access requests from private or internal network clients on a public network server.
    c) All dropped or denied access requests from private and public network clients to pass through the firewall that violate the security policy.
    d) All dropped or denied access requests from private and public network clients to send traffic to the firewall that violate the security policy.
    e) All attempts (successful or unsuccessful) of authentication at administrative or management interface.
    f) All access requests from public and private network clients to send traffic on the port(s) of the firewall used for administration/management.
    g) Startup of the firewall or its component that enforces the security policy.
    h) All manually entered changes in the firewall.

2) For each logged event, the following data elements shall be accurately recorded:-
    a) Date and time of event.

b) Protocol indicated in the IP field.
c) Source and destination IP addresses.
d) Source and destination port(s).
e) Message type.
f) Success or failure of authentication at administrative/management interface.

3) All log data shall be available on demand and be in a format readable to the user.
4) In the event of reapplication of electrical power after being lost or removed, the firewall shall:-
   a) Enforce the same security policy that was enforced prior to power loss, or apply a deny-all policy to ensure no unauthorized traffic is permitted.
   b) Ensure that all log data present in the firewall prior to power loss persists in the device.
5) The firewall shall not allow any unauthorized control of its administrative/ management functions.
6) That firewall shall be resistant to all known vulnerabilities that exist at time of development and known in the internet/public community. The firewall shall not introduce vulnerabilities in the network which it is meant to protect.
7) The firewall shall not allow any traffic to pass through other than that allowed by the security policy.
8) The firewall shall be resistant to trivial DoS attacks and shall fail closed if rendered inoperable due to DoS/ DDoS attacks for which there is no protection.
9) The firewall shall be capable of denying fragmented packets from passing through.
10) In addition to the above, **stateful inspection firewalls** shall also perform the following:-
   a) Keep track of each connection in a stable state.
   b) Track the state of connections and block packets that deviate from the expected state.
   c) Compare each new packet to the firewall state table to determine if the packet's state contradicts its expected state.
   d) For connectionless protocols such as UDP, packets shall still match an entry in the state table based on source and destination IP addresses and port information.

11) In addition to the above, **application firewalls** shall also perform the following:-

a) They shall contain an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviation.
b) Identification of unexpected sequences of commands such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent.
c) Input validation for commands, such as minimum and maximum lengths of arguments.
d) Enforce application state machines which check the compliance of traffic to the standard protocol in question.
e) Allow or deny access based on how an application is running over the network.
f) Block connections over which specific actions are being performed, e.g., allow or deny web pages that contain particular types of active content such as Java or ActiveX.

12) In addition to the above, **Next Generation Firewalls (NGFWs)** shall also perform the following:-
a) Apply application based security policies in addition to port based security policies.
b) Accurately identify applications on any port, identify diversified applications and different versions of the same applications as one application instead of multiple applications to identify upgraded applications.
c) Identify traffic specific to functions based on enterprise requirements; detect security risks of each function, and implement control and defense policies.
d) Identify not only the applications, but also the security risk to take protection measures. The predefined knowledge base of NGFW shall contain application signatures, potential security risks of applications and actions to mitigate these risks.
e) Support as many user authentication modes as possible, and the modes shall be consistent with the existing network access authentication mechanisms.
f) Inspect and filter the traffic that may contain sensitive information. NGFWs shall identify traffic based on flows to prevent evasion by fragmenting packets, identify file types to filter file contents, identify real file types and implement content filtering on files that have been compressed multiple times. Support for as many file types and protocols as possible shall be available.
g) Filter Word, Excel, PPT and PDF files transferred using email, HTTP, FTP and IM.

h) Identify access locations. By analyzing traffic information from the traffic map, NGFWs shall be able to determine the applications of abnormal traffic and determine whether these applications will cause security risks.

i) Have extra intelligence to enable users to migrate port-based policies to application-based policies easily.

j) The performance drop of NGFWs shall be lower than 40% with all security functions enabled.

3.3 Intrusion Detection and Prevention Systems (IDS/ IPS)

In addition to the General Requirements for ITSec equipment, Common Criteria and NIST Special Publication 800-94, following essential requirements shall also apply on IDS/IPS:-

1) IDS/IPS shall be designed to merge smoothly into the operational environment, making the sensors and management system simple to integrate and easy to use and configure.
2) IDS/IPS shall utilize a detection engine incorporating multiple technologies, including signature matching, protocol anomaly and behavior anomaly detection.
3) IDS/IPS shall have the ability to provide a “big picture” context of information about the network and its devices to qualify security information as well as speed analysis.
4) IDS/IPS shall be able to detect less critical threats, perform behavioral analysis and facilitate security forensics toolkits.
5) IDS/IPS shall perform centralized management and alerting capabilities across multiple devices.
6) IDS/IPS shall provide an analysis toolkit that efficiently drives policy refinement, and network security tools, especially firewalling, to simplify deployment.
7) IDS/IPS shall have visibility up to OSI layer 7 and shall employ deep inspection in order to identify illegal transactions and upended protocol states, buffer overflows and other suspicious activity.
8) IDS/IPS shall utilize behavioral analysis with tools to establish baselines, and to alert or block traffic when baseline deviations are detected.
9) IDS/IPS shall update threat signatures regularly and shall incorporate zero-day signatures as soon as they are announced.

3.4 DoS/DDoS Mitigation Systems

In addition to the General Requirements for ITSec equipment, Common Criteria and NIST Special Publication 800-189, following essential requirements shall also apply on DoS/ DDoS mitigation systems:-

1) High-rate DoS/ DDoS shall be mitigated by specialized hardware to withstand the load of attack while allowing legitimate traffic to pass through.
2) Network analysis shall be used to automatically and accurately distinguish attack traffic from legitimate traffic at OSI layers 3-7.
3) The DoS/ DDoS mitigation solution shall provide a defined process, which shall include published steps to mitigate attacks and escalation contact details.
4) The DoS/ DDoS mitigation solution shall be able to detect and mitigate the following types of attacks:-
    a) Volume based attacks
    b) Protocol attacks
    c) Application layer attacks
5) The DoS/ DDoS mitigation solution shall offer detection and mitigation of attacks at OSI layers 3 -7. The minimum threats shall include but not limited to:-
    a) ICMP floods
    b) SYN flood
    c) ACK flood
    d) Ping of death
    e) HTTP & HTTPS attacks
    f) Fragmented packet attacks
    g) DNS server attacks
    h) Smurf
    i) Teardrop
    j) Low-rate and permanent DoS attacks
    k) Peer-to-peer attacks
    l) Application level floods
    m) Zero-day DDoS attacks, preferably through manual inclusion of signature
6) The solution shall update DDoS threat signatures regularly in the monitoring and filtering devices.

7) The solution shall be able to automatically mitigate detected threats without requiring human intervention and shall provide notifications when attacks occur and are mitigated.
8) The solution shall allow for redirection of all incoming traffic on a specific IP address to filtering devices.
9) The solution shall provide statistics that are easily accessible. Statistics shall be available on demand or via portal based systems showing the level of DoS/ DDoS activity detected and mitigated.
10) The DoS/ DDoS mitigation solution should utilize redundant components and have its infrastructure availability > 99%.

3.5 Network Storage Systems

In addition to the General Requirements for ITSec equipment, Common Criteria and NIST Special Publication 800-209, following essential requirements shall also apply on network storage systems:-

1) All data stored in network storage systems shall be assigned a classification (public, confidential, secret, etc.) and shall use appropriate measures to ensure confidentiality, authenticity and integrity of the stored data.
2) Cryptographic algorithms and protocols used for confidentiality, authenticity and integrity of the stored data shall meet the requirements of GR for CP.
3) The network storage system shall identify the entities authorized to access the stored data and shall not allow access to unauthorized entities.
4) All users shall be assigned a unique user ID.
5) Data stored on the network storage system shall be easily accessible to authorized entities through the use of integrated search and index capabilities that can be quickly used to find data.
6) Backups of all data stored on the system shall be encrypted using appropriate mechanisms. Encryption keys shall be stored separately from the backup data.
7) All sensitive and/or classified data shall be encrypted during transit.
8) The network storage system shall use change detection mechanisms to record all changes in the system and shall log all attempted management events and transactions.
9) Each log entry shall include a timestamp, the source of log entry and a description of the event.
10) The network storage system shall use backup and replication techniques to ensure availability of data in event of failures.

11) Manual or automatic mechanisms shall be used to perform periodic data conversions and revalidations to assure integrity and authenticity of data to address data format or technological changes during lifespan of the stored data.
12) The network storage system shall provide appropriate measures against malwares, viruses, worms, rootkits, etc.
13) Storage traffic and normal server traffic shall be separated using physical or logical separation.
14) Management traffic shall be separated from all other network traffic and shall be protected using encryption.
15) Network access and protocols shall be filtered based on source IP address and all interfaces and LANs shall be segregated for security and performance.
16) Switches, extended routers and gateways shall be configured for least amount of access.

3.6 Smart Device

In addition to the requirements discussed in ***Chapter 6***, General Requirements for ITSec equipment, Common Criteria and NIST document NISTIR 8259, following essential requirements shall also apply to applications being used in smart device platforms such as Android, iOS, etc.

1) Adequate protection shall be built in to minimize the loss of sensitive data on the device. Data shall be properly classified and its protection, usage and storage shall be based on its classification.
2) When storing data on the device, file encryption shall be used to encrypt the data. The encryption algorithm shall meet the requirements stated in GR for CP.
3) Historical information such as GPS tracking data or other sensitive information shall not be stored on the device beyond its usage period.
4) Shall not use shared storage such as caches and temporary storage or public shared storage such as address book or media gallery to store sensitive information.
5) Passwords and other credentials shall be properly managed to avoid disclosure. Passwords shall never be stored in plaintext. Tokens shall be encrypted in transit using SSL/ TLS and shall be time bounded to the specific service and shall be revocable to minimize damage.
6) Swipe-based visual passwords are vulnerable to smudge attacks (using grease deposit on the screen to guess the password). Measures such as allowing repeated patterns shall be used to foil smudge attacks.

7) Passwords or Secrets shall never be stored in the application binary. Smart device application binaries are vulnerable and can be easily downloaded and reverse engineered.
8) Applications shall enforce the use of end-to-end secure channels such as SSL/ TLS when sending sensitive information over the internet. When using commercial applications, only certificates signed by trusted CAs shall be used.
9) To reduce the risk of MiTM attacks, a secure connection shall only be established after verifying the identity of the remote end device.
10) Adequate checks and controls shall be put in place to prevent unauthorized access to paid-for-resources.
11) Secure distribution practices shall be followed when distributing and installing applications on smart device.
12) When developing smart device applications, the following general coding best practices shall be strictly followed at a minimum:-
    a) Perform abuse case testing, in addition to use case testing.
    b) Validate all input.
    c) Minimize lines and complexity of code. A useful metric is cyclomatic complexity.
    d) Use safe languages (e.g. from buffer-overflow).
    e) Implement a security report handling point (address) security@example.com
    f) Use static and binary code analyzers and fuzz-testers to find security flaws.
    g) Use safe string functions, avoid buffer and integer overflow.
    h) Run apps with the minimum privilege required for the application on the operating system. Be aware of privileges granted by default by APIs and disable them.
    i) Don't authorize code/app to execute with root/system administrator privilege.
    j) Always perform testing as a standard as well as a privileged user.
    k) Avoid opening application-specific server sockets (listener ports) on the client device. Use the communication mechanisms provided by the OS.
    l) Remove all test code before releasing the application.
    m) Ensure logging is done appropriately but do not record excessive logs, especially those including sensitive user information.

3.7 Cloud Based Services

In addition to the General Requirements for ITSec equipment, requirements listed by State Bank of Pakistan for Cloud Service Providers (CSPs), Common Criteria and NIST Special

Publication 500-322, following essential requirements shall also apply to information systems being used to provide cloud based services:-

1) Strong authentication methods, such as two-factor authentication shall be used to access the cloud service. Strong passwords shall be chosen for each account and shall be different for different accounts.
2) A policy shall be formulated and implemented for accessing accounts in the cloud systems.
3) User names and passwords shall be protected by using adequate methods. User shall ensure that passwords are kept in a safe place and not stored in the device in plain form. Password saving in web browsers and applications shall also be explicitly turned off. The cloud service shall be logged off when not in use.
4) Protection mechanisms such as encryption, integrity checking, etc., shall be used to protect data in transit or being stored in the cloud architecture. Stored data shall only be accessible to authorized entities. Algorithms used for encryption, authentication and integrity shall meet requirements stated in GR for CP.
5) Only trustworthy devices shall be used when accessing cloud services. The device shall be physically secured and use access control mechanisms.
6) Backups of data stored on the cloud shall be routinely updated to ensure data availability in case of failure/ malfunction of cloud service.

Chapter 4

Information Security Auditing & Screening of ICT Infrastructure

4.1 Introduction

Majority of ICT equipment being used in government organizations and institutions is purchased from foreign vendors without any preliminary assessment or screening at time of induction. ICT infrastructure may contain vulnerabilities which may be intentional, in the form of bugs, malwares, Trojans, etc., or unintentional, due to some misconfiguration or lack of proper quality assurance at time of development. These vulnerabilities may enable entities to steal, monitor or modify information being handled by the ICT systems and therefore impose a serious risk to the organization using these systems.

Government/ Sensitive organizations are required to protect security of their valued and critical information systems/ networks/ assets. Such organizations are desired to implement necessary safeguards designed to adequately protect these essential assets. Instead of relying on reactive auditing post a security breach, a regular internal as well as external audit and penetration testing framework is required to be introduced. As a proactive measure, a team of concerned organization and NTISB designated team is suggested to initially perform an internal audit prior engaging a security cleared Penetration Testing Private Firm. Penetration testing will facilitate in obtaining evidences of the efficacy of implemented Security Policies (SP) in order to maintain Integrity, Confidentiality and Availability (ICA) of critical assets by ensuring that:-

1) Systems/ networks are responding to the latest risks/ threats
2) Systems are configured in accordance with current SP
3) Organization reassesses the information security of its systems/ networks as new vulnerabilities are discovered

NTISB in consultation with relevant stake holders (including pkCERT) will devise a process for firm(s) registration and their security clearance intended to perform audit(s).

4.2 Organizational Assistance Program

To support public and critical private sector organizations for improving security of their IT infrastructure, NTISB will facilitate conduct of INFOSEC assessment through formulation of joint teams. In case of cyber/ INFOSEC compromise, a special and targeted audit will be

conducted to ascertain threat actor, entry point, extent of damage and recovery options etc. Foremost components of the audit program includes:-

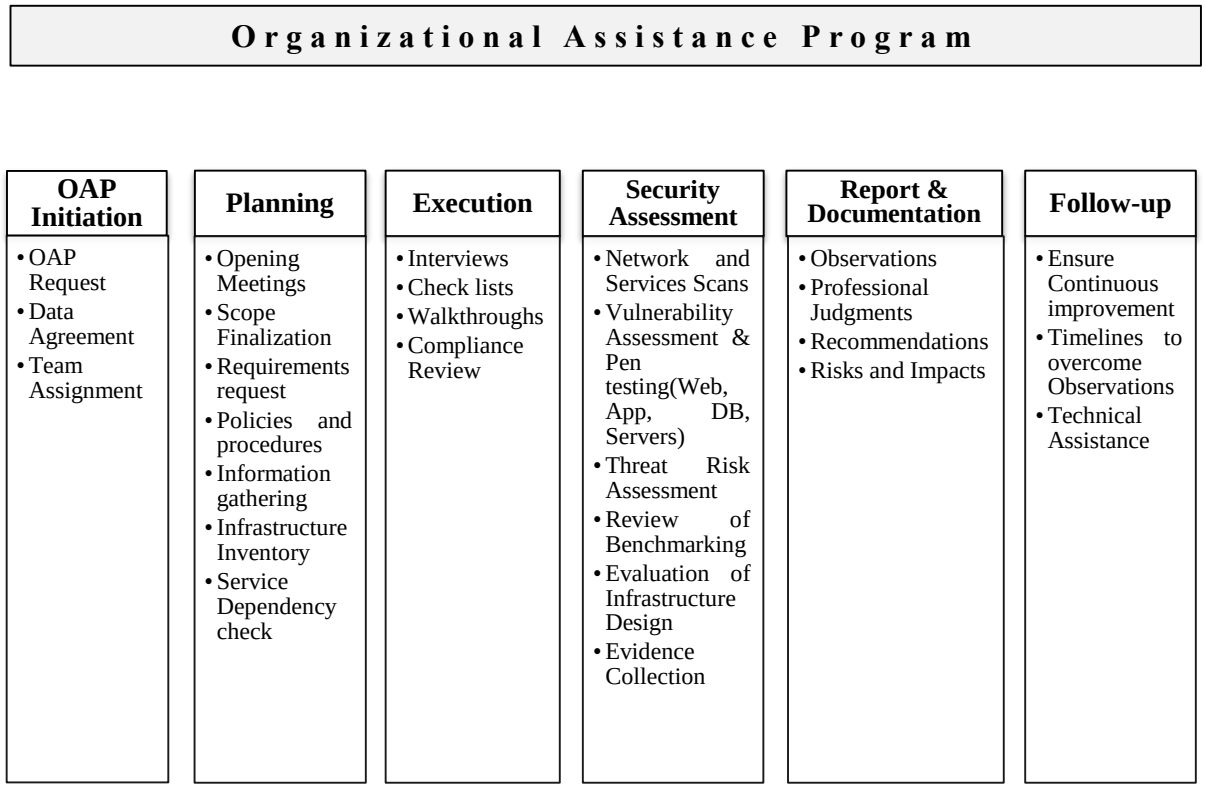

Figure 4.1: Organizational Assistance Program

4.3 Audit Scope

Controls as depicted below will include scope of the testing whether internal or external.

Figure 4.2: Audit Scope

4.4 Proposed Audit Framework

In proposed framework, the internal audit will be conducted by the joint team of experts from the organization and NTISB designated team (including reps from pkCERT) who will define the scope of audit and agree on the controls for which penetration testing will be performed. The external audit of the system/ network will be conducted subsequently by an independent security cleared company. The audit report of both the audits will be compared and assessed by a NTISB Technical Evaluation Committee (TEC) to take/ decide corrective actions and remedial measures for overcoming the weaknesses highlighted in both reports.

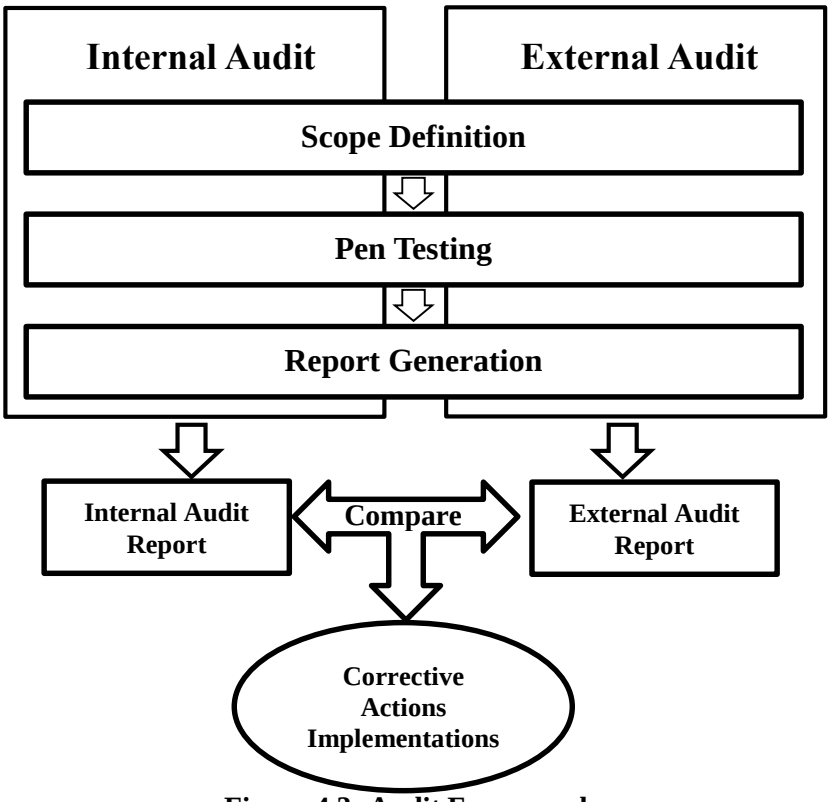

Figure 4.3: Audit Framework

Proposed framework intends to assist the organization in following three ways:-

1) Precisely determine what should be protected (the assets) and their weaknesses (vulnerabilities) involved in their daily activity.
2) Assess what vulnerabilities can be exploited by an attack as well as the threats that might be materialized in an attack.
3) Evaluate the efficiency and the effectiveness of the policy and controls implemented in order to evaluate if they are being correctly implemented or if they need any adjustment.

It is important that ICT infrastructure or any component (hardware or software) be screened in addition to auditing for vulnerabilities at time of induction into any organization. All

government organizations and institutions desirous to induct ICT equipment shall ensure that the equipment formally goes through the auditing and screening process through NTISB.

4.5 The Audit Process

The Audit (internal/ external) will be conducted in three distinct phases as shown in figure 4.3.

4.5.1 Phase 1 – Scope Definition Meeting

This phase will be comprised of two or three meetings between the Auditor and the Auditee and suggested to be completed within 2x weeks. Following activities are envisaged in this phase:-

1) Identification of contact individuals from both side
2) Define the scope, approach and methodology
3) Agree to specific test cases and possible attack paths to be exploited

4.5.2 Phase 2 – Penetration Testing

In this phase, the auditor will actually carry out the penetration testing of the controls selected in first phase to detect exploitable weak points in the system. This phase is suggested to be completed within 3 ~ 4 weeks depending on the Auditee system/ network/ scope defined.

4.5.3 Phase 3 – Report Preparation

In the third and final phase of the audit, the auditor will prepare a report of the audit conducted along with all the findings and associated risks/ vulnerabilities discovered during penetration testing, suggest remedial measures and corrective actions for them. This activity will be completed within 2x weeks.

4.5.4 Corrective Actions Implementation

This is the culminating point of auditing that will identify implementation aspects of the recommendations contained in internal and external audit reports.

4.6 Screening Process

Supply Chain Attacks are favorite accessibility method into intractable organizations. These attacks are launched by infecting the equipment purchased by targeted organizations with malware, remote intrusion systems and discreet bugging devices etc. It is therefore imperative to adopt ways and means to safeguard against such attacks. Screening is post–procurement, pre-deployment verification of software, IT and electronic equipment as well as non-electronic

items being inducted into organization which necessitates 100% testing (preferably) of equipment under a special mechanism. Essentially, equipment belonging to sensitive organizations and officials (atleast) shall be screened as per policy devised by NTISB.

The screening process will vary depending on the type, purpose and use of IT infrastructure and sensitivity of the information contained or processed. In broad terms, ICT equipment may be classified into the following:-

1) ICT Hardware – devices with no embedded firmware or software
2) ICT Software/Firmware – including software applications and firmware embedded in hardware devices
3) Network Devices – including routers, switches, firewalls, IDs/IPS, etc.
4) Network Management Policies – include management of network, network design and configuration, physical security & resilience, connecting devices to the network etc.

4.6.1 Screening of ICT Hardware

All ICT hardware shall be screened to detect any electronic/ hardware bugs. These bugs have the same general specification irrespective of the nature of equipment in which they are planted. The equipment shall be placed inside an environment free from external RF radiation. Suitable test equipment shall be used to detect any unwanted transmissions emanating from the equipment.

4.6.2 Screening of ICT Software/ Firmware

Bugs, viruses, malwares and backdoors may be present inside software applications and firmware residing in PCs, laptops, network devices such as firewalls, switches, routers, IDS/ IPS, etc. Complete assurance requires complete source code of the software and/ or firmware of the application and equipment alongwith extensive programming skill set to analyze the code. In the absence of the source code, only a certain level of confidence can be attained. Therefore, the scope of testing shall vary depending upon the availability or otherwise of the source code.

Software applications also include operating systems inside PCs and laptops; database applications, antivirus applications and hardware specific applications that may be required to operate a particular hardware device. To determine whether software applications contain vulnerabilities that can be exploited, thorough application security testing and examination shall be carried out. Wherever possible, code walkthrough will be resorted for gaining preliminary insight into the working of software/ firmware.

4.6.3 Screening of Network Devices

Techniques used to screen network devices include review of documentation, logs, rule-set and system configuration, file integrity checking, network sniffing and penetration testing. Documentation review shall be carried out to determine if the technical aspects of the device, its policies and procedures are current and comprehensive. Network sniffing shall be used to check for unwanted open ports and any unsolicited traffic entering or exiting these ports, decode protocols and examine headers and payloads to flag information of interest. Finally penetration testing shall be performed to determine vulnerabilities that might enable an unauthorized entity to gain access to the system.

Chapter 5

Public Key Infrastructure (PKI) Security

5.1 Introduction

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies and procedures which are used to create, manage, distribute, use, store, and revoke digital certificates through a Certification Authority (CA). These digital certificates are based on cryptography and comply with the X.509 v3 standard. Electronic Transactions Ordinance 2008 (ETO) was issued to provide legal coverage to electronic transactions. It provides a legal framework to recognize and facilitate documents, information, communication and transactions in electronic form by incorporation of digital signatures.

Digital certificates will be issued to end users, IT systems, applications and services developed, inducted and used within government/semi-government systems and networks by proving the identity electronically/ digitally.

ECAC grants or renew accreditation to PKI service providers, their services and security procedure. For the purpose, NTISB will facilitate in cryptographic strength evaluation of offered PKI services by Certification Service Providers. Based upon the NTISB provided report, ECAC will issue accreditation certificate according to its applicable regulations/ procedures.

5.2 Security of PKI Architecture

The PKI architecture involves core PKI components and their integration with various applications and services along with the placement of appropriate physical and logical security controls.

5.2.1 Core Components Security Requirements

PKI may consist of following core components which shall perform dedicated functions:-

1) **CA Server**. CA (Root, Intermediate, or Issuing) server shall issue and revoke certificates.
2) **Certificate Revocation List (CRL) Server**. CRL server shall host the digitally signed list of revoked certificates issued by the CA.

3) **Online Certificate Status Protocol (OCSP) Server**. OCSP Server shall provide a digitally signed response regarding certificate's status.
4) **Simple Client Enrollment Protocol (SCEP) Server**. SCEP server shall provide remote certificate enrollment on behalf of Certificate Authority to X.509 v3 compliant and intelligent network devices.
5) **Certificate Enrollment Terminals (CET)**. Desktop PCs with attached smart card readers to perform certificate personalization & enrollment.

5.2.2 Physical Security Requirements

1) All the Servers (CA, CRL, OCSP and SCEP) of a particular Central Location or individual building shall be placed in dedicated racks with the keys accessible to the authorized personnel only.
2) Racks shall be placed in separate locked room with biometric access control.
3) The operational environment of CA and CETs shall be monitored by 24/7 CCTV monitoring system with 90x days backup.

5.2.3 Logical Security Requirements

1) CA servers (Root, Intermediate, and Issuing) along with the CETs shall be placed in the offline/ air-gapped state/ network.
2) CRL, OCSP and SCEP servers shall be placed in the De Militarized Zone (DMZ) accessible to the organizational applications & servers only.
3) Multi-factor Authentication (Smart Card & PIN) for Access Control of CA servers.
4) Two-Person Secret Sharing Access Control mechanism shall be provided for issuance of digital certificates.

5.2.4 Certificate Security Requirements

Certificates are generated using underlying cryptographic public key algorithm, refer to GR for CP for specific CP requirement.

1) CAs will issue certificates with RSA-4096 bit key length or with similar strength CP.
2) Applications & server certificates will be issued with RSA-2048/4096 bits key length or with similar strength CP.
3) User smart card certificates will be issued with RSA-2048 bits key length or with similar strength CP.

5.2.5 Hardware Requirements

To fulfill above mentioned security requirements, following is the minimum requirement of technical hardware for PKI certificate issuer that should commensurate with the function, load, throughput, security and such other functional and performance related requirements of a PKI service:-

1) CA Server
2) CRL Server
3) OCSP Server
4) SCEP Server
5) Certificate Enrollment Terminals
6) Smart Card Readers
7) Smart Cards
8) Biometric Access Control
9) CCTV Cameras
10) Backup Server
11) Network Switches
12) Firewalls
13) Hardware Security Modules

Chapter 6

Secure Software Application

6.1 Introduction

Any piece of source code or a complete software (desktop, web or mobile app) providing cryptographic services is considered as secure software. This chapter provides a basis for verifying secure software application's technical security controls as well as any technical security controls in the environment that are relied on to protect against known vulnerabilities. The scope of the verification includes all code that was developed or modified in order to create secure software or release.

6.2 Architecture, Design and Threat Modeling

Following shall be implemented by developer and verified by evaluator:-

1) All secure software components are identified and known to be needed.
2) Security controls are never enforced only on the server side, but also on the respective remote endpoints or clients.
3) A high-level architecture for the secure software and all connected remote services has been defined and security has been addressed in that architecture.
4) Data considered sensitive in the context of the secure software is clearly identified.
5) All secure software components are defined in terms of the business functions and/or security functions they provide.
6) A threat model for the secure software and the associated remote services has been produced that identifies potential threats and countermeasures.
7) All security controls have a centralized implementation.
8) Cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow key management standard (GR for KMS).
9) A mechanism for enforcing updates of the secure software exists.
10) Security is addressed within all parts of the software development lifecycle.
11) A responsible disclosure policy is in place and effectively applied.
12) Secure software should comply with privacy laws and regulations.

6.3 Data Storage and Privacy

Following shall be implemented by developer and verified by evaluator:-

1) System credential storage facilities need to be used to store sensitive data, such as Personal Identifiable Information (PII), User Credentials or Cryptographic keys.
2) No sensitive data should be stored outside of the secure software container or system credential storage facilities.
3) No sensitive data is written to application logs.
4) No sensitive data is shared with third parties unless it is a necessary part of the architecture.
5) The keyboard cache is disabled on text inputs that process sensitive data.
6) No sensitive data is exposed via Interrupt Procedure Calls (IPC) mechanisms.
7) No sensitive data, such as passwords or pins, is exposed through the user interface.
8) No sensitive data is included in backups generated by the secure software.
9) Secure software removes sensitive data from views when moved to the background.
10) Secure software does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.
11) Secure software enforces a minimum device-access-security policy, such as requiring the user to set a device passcode.
12) Secure software educates the user about the types of personally identifiable information processed as well as security best practices the user should follow in using the software.
13) No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote endpoint or secure storage when needed and only be kept in memory.
14) If sensitive data is still required to be stored locally, it should be encrypted using a key derived from hardware backed storage which requires authentication.
15) Secure software local storage should be wiped after an excessive number of failed authentication attempts.

6.4 Cryptographic Security

For security requirements of approved cryptographic algorithm, key size and protocols refer to GR for CP for security grading of CP employed in software. General cryptographic requirements are defined as below:-

1) Secure software does not rely on hardcoded keys as a sole method of encryption.
2) Secure software uses proven implementations of Cryptographic Primitives.

3) Secure software uses Cryptographic Primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.
4) Secure software does not use Cryptographic Protocols or Algorithms that are widely considered deprecated for security purposes.
5) Secure software doesn't re-use the same cryptographic key for multiple purposes.
6) All random values are generated using a sufficiently secure random number generator (Refer to GR for SDI and GR for KMS).

6.5 Authentication and Session Management

Authentication and sessions can be managed in number of possible mechanism, only basic requirements are defined here but developer should consult latest and up to date literature for best known secure authentication and session management.

1) If secure software provides users access to a remote service, some form of authentication, such as username/ password (essentially) and/ or certificate based authentication (i.e. Multi-Factor Authentication, MFA preferably) etc. is performed at the remote endpoint.
2) If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.
3) If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.
4) The remote endpoint terminates the existing session when the user logs out.
5) A password policy exists and is enforced at the remote endpoint.
6) The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.
7) Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.
8) Biometric authentication, if any, is not event-bound (i.e. using an API that simply returns "true" or "false"). Instead, it is based on unlocking the keychain/keystore.
9) As stated previously, a second factor of authentication exists at the remote endpoint and the MFA requirement is consistently enforced.
10) Sensitive transactions require step-up authentication.
11) Secure software informs user of all sensitive activities with their account. Users are able to view a list of devices, view contextual information (IP address, location, etc.), and to block specific devices.
12) Authorization models should be defined and enforced at the remote endpoint.

13) All authentication decisions should be logged.

6.6 Network Communication

In addition to the network security requirements listed in ***Chapter 3*** following shall be implemented:-

1) Data is encrypted on the network using TLSv1.3 or above or latest protocols. The secure channel is used consistently throughout the secure software components.
2) TLS (Latest protocols) settings are in line with current best practices, or as close as possible if operating system does not support the recommended standards.
3) Secure software verifies X.509v3 or above certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.
4) Secure software either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.
5) Secure software doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.
6) Secure software only depends on up-to-date connectivity and security libraries.

6.7 Platform Interaction

While communicating across different platforms following should be taken care of while data is being transmitted:-

1) Secure software only requests minimum set of necessary permissions.
2) All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the User Interface (UI), IPC mechanisms such as intents, custom URLs, and network sources.
3) Secure software does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.
4) Secure software does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.
5) JavaScript is disabled in WebViews unless explicitly required.
6) WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file etc. are disabled.
7) If native methods of the secure software are exposed to a WebView, verify that the WebView only renders JavaScript contained within the software package.

8) Object deserialization, if any, is implemented using safe serialization APIs.
9) Secure software protects itself against screen overlay attacks.
10) A WebView's cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed.
11) Verify that secure software prevents usage of custom third-party keyboards whenever sensitive data is entered.

6.8 Code Quality and Build Settings

1) Secure software is signed and provisioned with a valid certificate (of which the private key is properly protected) or similar mechanism ensuring integrity.
2) Secure software has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).
3) Debugging symbols have been removed from native binaries.
4) Debugging code and developer assistance code (e.g. test code, backdoors, hidden settings) have been removed. Secure software does not log verbose errors or debugging messages.
5) All third party components used by the secure software, such as libraries and frameworks, are identified, and checked for known vulnerabilities.
6) Secure software catches and handles possible exceptions.
7) Error handling logic in security controls denies access by default.
8) In unmanaged code, memory is allocated, freed and used securely.
9) Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, or similar features by other platforms are activated.

6.9 Resiliency against Reverse Engineering Requirements

First attempt made by attacker is reverse engineering of source code, developer preferably develop mechanisms to resist and slow down reverse engineering of source code by adapting following guidelines:-

1) Secure software detects and responds to:-
    a) The presence of a rooted or jailbroken device either by alerting the user or terminating application.
    b) Debugger being attached by detecting debugging. All available debugging protocols must be covered.
    c) Tampering with executable files and critical data within its own sandbox.

d) The presence of widely used reverse engineering tools and frameworks on the device.

e) Being run in an emulator.

f) Tampering the code and data in its own memory space.

2) The detection mechanisms trigger responses of different types, including delayed and stealthy responses.

3) Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.

4) Secure software implements a 'device binding' functionality using a device fingerprint derived from multiple properties unique to the device.

5) All executable files and libraries belonging to secure software are either encrypted on the file level and/ or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.

6) If the goal of obfuscation is to protect sensitive computations, an obfuscation scheme is used that is both appropriate for the particular task and robust against manual and automated de-obfuscation methods, considering recent published research. The effectiveness of the obfuscation scheme must be verified through manual testing. Note that hardware-based isolation features are preferred over obfuscation whenever possible.

7) As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.

Chapter 7

BlockChain & Virtual Currency Based Assets

7.1 Introduction

BlockChain (BC) has enabled a novel paradigm for managing digital trust and ownership in partial- or zero-trust environments. BC uses tokens to conduct transactions, exchange verifiable data and achieve coordination across organizations and on the web. BC enables users to independently control token custody in digital wallets through public-key cryptography and interact with one another in a client-to-client manner. The term "Virtual Current Based Asset" refers to any programmable digital representation of value that can be digitally traded, transferred or used for payment. BC based crypto currencies (e.g. Bitcoin, Ethereum, Tether, etc.) and digital currencies (e.g. e-money, e-paisa, gaming coins, etc.) are some known examples of virtual assets. Virtual Asset security requirements are for all information systems that make use of virtual assets including exchanges, web applications, and virtual asset storage solutions.

Requirements in this document are stipulated to complement international information security standards (i.e. ISO 27001, PCI-DSS, etc.) and best practices. These requirements are not developed to substitute or replace existing security standards and will be read in conjunction with guidelines and recommendations already published by Financial Monitoring Unit (FMU) of State Bank of Pakistan (SBP), Financial Action Task Force (FATF) and Crypto Currency Certification Consortium (C4).

7.2 Applicability

These requirements shall be applicable to any information system that make use of a Virtual Asset. This includes (but is not limited to) Virtual Asset Exchanges, Virtual Asset Marketplaces, Virtual Asset Games, Virtual Asset Processors and Virtual Asset/ Cryptographic Storage. Furthermore, as is the case with the countries with legal virtual asset based transaction mechanism, it is the understanding of this standard that virtual currency based business or transactions will be developed or legalized in Pakistan through a mechanism more or less similar to below outline:-

1) 'Digital exchanges' that convert digital currency into fiat currency are equated as Banks and regulated by **SBP**.

2) 'Websites' and 'Mobile' apps that sell products or provide services on internet (**TOR, VPN**, **WWW, etc.)** be equated as '**BUSINESSES'** and regulated by **SECP**, **FBR** and **PTA** (for provision of client IPs doing transactions).
3) 'Digital wallets' that contain 'private key' and 'digital currency' of an identity be registered against **CNIC** with **NADRA** and **SBP** in the same way as **KYC** (Know Your Client) is managed by Banks.
4) Business will be conducted after Cryptographic Certification by **NTISB**.

7.3 Virtual Asset Security Requirements.

To manage cryptographic requirements for making use of virtual assets, 8x security aspects of information systems involving Virtual Assets are further organized into 3x sub-domains as below:-

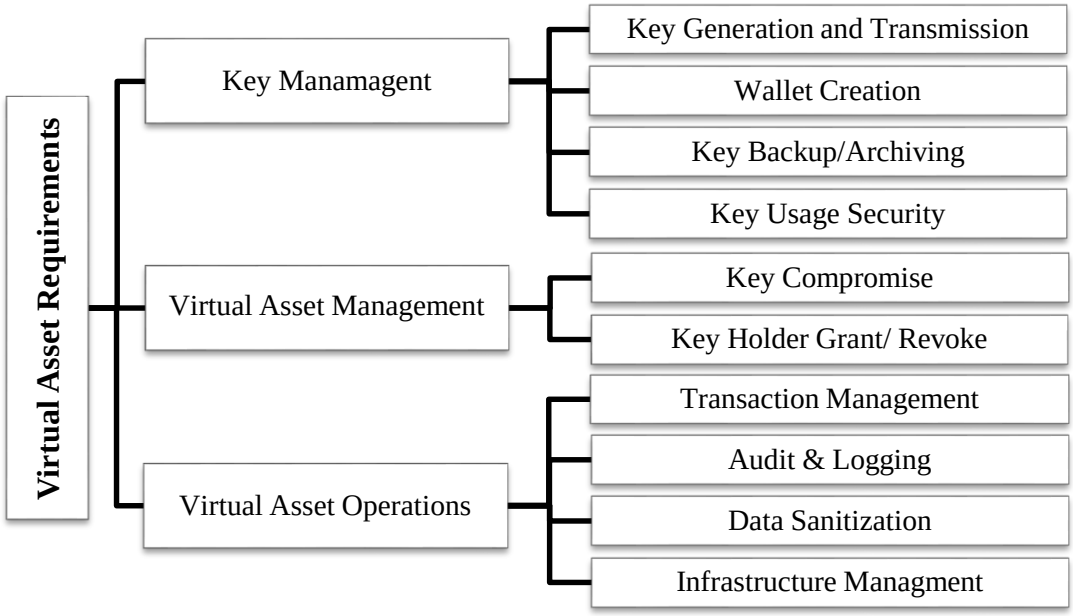

Figure 7.1: Virtual Asset Requirements

7.3.1 Wallet and Key Management

In addition to the applicable requirements listed in GR for KMS following should be applicable to Key Management of Virtual Assets:-

7.3.1.1. Key Generation and Transmission

1) Key or seed generation methodology shall be validated prior to use and administrator of the system shall generate the key/ seed on a cryptographically strong offline system.

2) The cryptographic keys and seeds shall be created on a system with sufficient entropy (i.e. conforming to NIST SP800-90B) to ensure that the keys are not created with any bias towards a reduced range of values, or other deterministic properties.
3) Key/ Seed Generation software shall be free from any features that restrict the generated seed to conform to deterministic values and features that store or transmit the generated seed to another actor except where such features enhance the effective security of the software (e.g. DRBGs).
4) A digital signature shall be generated and published for the software. The signature shall be validated prior to each execution.
5) In cases where keys or seeds are created without the use of software, the creation methodology shall be validated to ensure non-determinism.
6) If the key or seed is generated using a Deterministic Random Bit Generator (DRBG) then it shall conform to NIST SP 800-90A and shall be seeded with at least two separate cryptographically secure sources of entropy that have been combined in a cryptographically secure manner. The Dual_EC DRBG from NIST SP 800-90A shall not be used for the purpose.
7) The generated key/ seed shall be transferred securely onto the target device and then securely deleted using standard data sanitization techniques to protect the confidentiality of the key/ seed.
8) The key/ seed shall be transmitted and stored in a strongly encrypted format for backup.

7.3.1.2. Wallet Creation

1) A new address for every transaction shall be generated and assigned deterministically based on seeds that are kept private. This will be linked with an identity of a person i.e. CNIC and should be registered with **NADRA** and **SBP** in the same way as KYC (Know Your Client) is managed by **Banks**.
2) In addition to requirements mentioned in para 3.1 of NIST-IR 8301, these requirements apply to self-hosted wallets, custodian wallets and smart contract vaults.
3) The address generated by a wallet shall require a minimum of two signatures in order to complete.
4) Redundant keys shall be assigned to each wallet for recovery purposes.
5) Any keys that have signing authority on a single wallet shall be stored in different locations by multiple organizational entities.

7.3.1.3. Key Backup/ Archiving

1) Cryptographic keys and/ or seeds shall be stored in encrypted form when not in use and a backup shall exist for at least as many keys as is required to spend funds in encrypted form.
2) A secure backup protected by temper-evident mechanism(s) and appropriate access controls (i.e. MFA) of the cryptographic key/ seed shall exist.
3) The backup shall be stored in a location that is resistant to electromagnetic interference, geographically separate from the usage location of the primary key/ seed and protected against environmental risks (e.g. fire, flood, etc.)

7.3.1.4. Key Usage Security

1) Access to the primary key/ seed shall require an identifier (e.g. username, email, GUID, etc.) and at least two-factor authentication.
2) All keys/ seeds shall only be used in trusted environments.
3) All key/ seed-holders shall have their references checked and undergone identity verification prior to being trusted to hold one of the organization's keys/ seeds.
4) No two master keys/seeds of the same multi-signature wallet shall be present on the same device.
5) Digital signatures shall use a 'k' value that is never repeated.
6) Verification of fund destinations and amounts shall be performed via authenticated communication channel prior to key/ seed use.

7.3.2 Virtual Asset Management

7.3.2.1. Key Compromise

1) An inventory of all keys/seeds shall exist in the organization.
2) Proper Key Compromise Protocol outlines shall be developed covering each specific class of key used throughout the system along with a detailed plan of dealing with its compromise including the proper use of Authenticated Communication Channels during execution.
3) Tests of the Key Compromise Protocol shall be executed regularly to confirm the viability of the procedures and to ensure staff remain trained to use them in case of a compromise.

7.3.2.2. Key Holder Grant/Revoke

1) Adequate access control policies and procedures shall be developed when on-boarding or off-boarding staff from keyholder positions within the organization.

2) "Least Privilege Principles" shall be applied to the information system as well as necessary access where required.
3) All keyholder grant/ revoke requests shall be conducted over Authenticated Communication Channels.

7.3.3 Operation Management

7.3.3.1. Transaction Management

No additional requirement to para 4 of NIST IR-8301.

7.3.3.2. Audits and Logging

1) **Digital exchanges** that convert digital currency into fiat currency should be audited as Banks and regulated by **SBP**.
2) **Websites** that sell products or provide services whether on TOR or on WWW should be registered and audited as 'BUSINESSES' and regulated by **SECP**, **FBR** and **PTA** (for provision of client IPs doing transactions).
3) Regular security audits and/ or penetration/ vulnerability tests shall be performed on a defined schedule of at least once per calendar year.
4) A developer who is knowledgeable about cryptographic security shall assist in the design and implementation of the information system involving use of virtual assets.
5) Audit trails shall exist for a subset of actions that are performed within the information system and all actions by all users shall be logged and correlated.
6) Audit information shall be regularly backed up to a separate server.

7.3.3.3. Data Sanitization

1) An audit trail shall be maintained for every piece of sanitized media.
2) A detailed policy outlining the requirements for sanitization of digital media that holds/ held Virtual Asset keys shall be developed.
3) Understanding by all staff who have access to cryptographic keys shall be ensured via awareness trainings and posters to be aware of how data persists on digital media after deletion.

7.3.3.4. Infrastructure Management

No additional requirement to para 5 of NIST IR-8301.

Chapter 8

Indigenous Development & Export of ITSec Equipment

8.1 Introduction

Indigenous Information Assurance/ Cryptographic/ ITSec solutions are offered by private sector companies as well as public establishments for protection of information systems/ networks. For use within country, indigenously developed INFOSEC product, service, criteria etc. will be **preferred**. In pursuit of **knowledge based economy** development and benefiting from such niche technologies, **export** of these solutions present a desirable opportunity for **securing foreign exchange**; however, **sensitivities related with ITSec exports warrant restrictions** that should be applied on export of such systems.

8.2 Export of ITSec Equipment

Following points should be taken into consideration while applying for export of ITSec equipment:-

1) Export of ITSec solutions that remained under use or are currently in use or are under evaluation or are under consideration for Government, Armed forces or Critical National Infrastructure (CNI) is prohibited.
2) Export of solutions that have neither been evaluated by NTISB nor used by Government, Armed Forces or CNI may be allowed but after evaluation by NTISB for sole purpose of "ITSec Export Evaluation".
3) Till such time that "ITSec Export Evaluation" requirements are finalized, clause 5.2 (1) and 5.2 (2) shall be applicable.
4) Export of ITSec Solutions offer opportunity for exploitation with regards to system details/ information of similar solutions under use of Government/ Armed Forces/ CNI. It is therefore, only in presence of necessary safeguards/ variations that such devices will be cleared for export subject to assessment through ITSec Export Evaluation.
5) For detailed instructions, Developers/ Vendors must approach NTISB beforehand for obtaining current guidelines, procedures and regulations on ITSec exports.
6) ITSec Export Evaluation will be financed by Developer/ Vendor.

All local firms engaged in Research & Development/ production of ITSec solutions shall register themselves with NTISB and/ or Ministry of Defense Production. In collaboration with Pakistan Software Export Board (PSEB), NTISB will facilitate private industry in export.

Annex 'A'

PSS Gazette Notification

REGISTERED No. M - 302 / L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, THURSDAY, JUNE 22, 2023

PART II

Statutory Notifications (S.R.O.)

GOVERNMENT OF PAKISTAN

MINISTRY OF SCIENCE AND TECHNOLOGY

NOTIFICATION

Islamabad, the 14th June, 2023

S. R. O. 762(I)/2023.—In exercise of the powers conferred by section 14 of the Pakistan Standards and Quality Control Authority Act, 1996 (VI of 1996), the Federal Government in consultation with the Pakistan Standards and Quality Control Authority is pleased to:—

(a) prohibit with effect from **1st June, 2028,** the manufacture, storage and sale of the articles specified in column (2) of the Schedule below for sectors requiring cryptographic and IT security systems to protect sensitive information in computer, telecommunication or cyber systems which do not conform to the Pakistan standards established by the Pakistan Standards and Quality Control Authority as mentioned in column (3) of the Schedule;

(b) direct that each such article which conforms to the Pakistan Standards relating to that article shall be marked with standard mark of the Authority specified in column (3) of the Schedule, namely:—

(1853)

Price: Rs.5.00

[1196(2023)/Ex. Gaz.]

SCHEDULE

Sr.No	Description of article	Pakistan standard
(1)	(2)	(3)
1.	**IT Security**. Such articles that claim provision of a specific cyber security function such as all kinds of firewalls, network routers, high capacity switch, intrusion detection and prevention, end point security, secure access control systems, security information management, security information and event management, secure operating systems, secure applications, secure database management, anti-denial of service, anti-virus, anti-spyware, anti-theft, anti-malware or any other such solution.	PS:5543 Pakistan Security Standard for Cryptographic & ITSec Devices- ITSec Guide Book
2.	**Cryptographic**. Such articles that claim provision of confidentiality, integrity, authentication, availability or non-repudiation to users, networks or systems such as all kinds of cryptographic encryptors, hardware security modules, key generation, management or distribution systems, cryptographic tokens or systems for secure access or user authentication, cryptographic algorithms or protocols or operations, cryptography based communication or web applications, secure Virtual Private Networks or other such solutions.	PS:5544 Pakistan Security Standard for Cryptographic & ITSec Devices- Crypto Guide Book;

(c) direct that sectors requiring immediate adoption for deployment may undertake appropriate actions at their level with consultation of respective regulators or PPRA; and

(d) direct that consumer electronics or IT systems or solutions that do not claim the provision of security functionality shall stand excluded from this Notification.

[F. No. 5(87)/2021-ATA-II.]

AMIR MUHAMMAD KHAN NIAZI,
Deputy Secretary (Admn).

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.