SWIFT

PCI DSS COMPLIANT

الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

Ramadan Ahmed
VP & Regional Head, Information Security Governance

SWIFT, PCI-DSS, NESA

01 October 2022

Agenda

- **SWIFT**
  - Swift Cyber Heist
  - SWIFT Overview
  - How Swift Work
- **PCI-DSS**
  - Cyber breaches
  - PCI-DSS overview
  - How Cards work
- **NESA**
  - NESA UAE IA Overview
  - Questions & Answers

SWIFT Customer Security Controls Framework (CSCF)

SWIFT CYBER HEIST 5 BREACHES

The Bank of Bangladesh $951,000,000 stolen using trusted Windows Software

In February 2016, the Bank of Bangladesh faced a major cyber attack resulting in $81,000,000 unrecovered. The attackers gained control over SWIFT systems by deploying trusted Windows software to the bank's internal systems. Potentially, $951,000,000 was at stake.

Far Eastern International Bank in Taiwan $60 Million using tailored Malware

In October 2017, the bank in Taiwan was the target of a bank heist involving almost $60 million. The hackers reportedly used tailored malware to generate SWIFT messages containing fraudulent information. Much of the stolen funds was recovered with help of its banking counterparts, however $500,000 remained untraceable.

Banco del Austro in Ecuador $12,000,000 stolen with credential compromise

In January 2015, attackers obtained the credentials of a bank employee and used these to access the employee's email account to alter SWIFT transfer requests. Transfers were made from several accounts of Wells Fargo, HSBC and Hang Seng Bank accounts totaling $12 million. In the course of the investigation however, $1.85 million dollars were recovered and returned.

Banco de Chile in Chili $10,000,000 stolen using Buhtrap its MBR Killer malware

A destructive malware was released at the Banco de Chile in May 2018. It caused mayhem, distracting defenders from another attack on the crown jewels. Whilst all systems were down, fraudulent messages were sent for $10,000,000.

A Russian bank has spotted attacks targeting its SWIFT systems

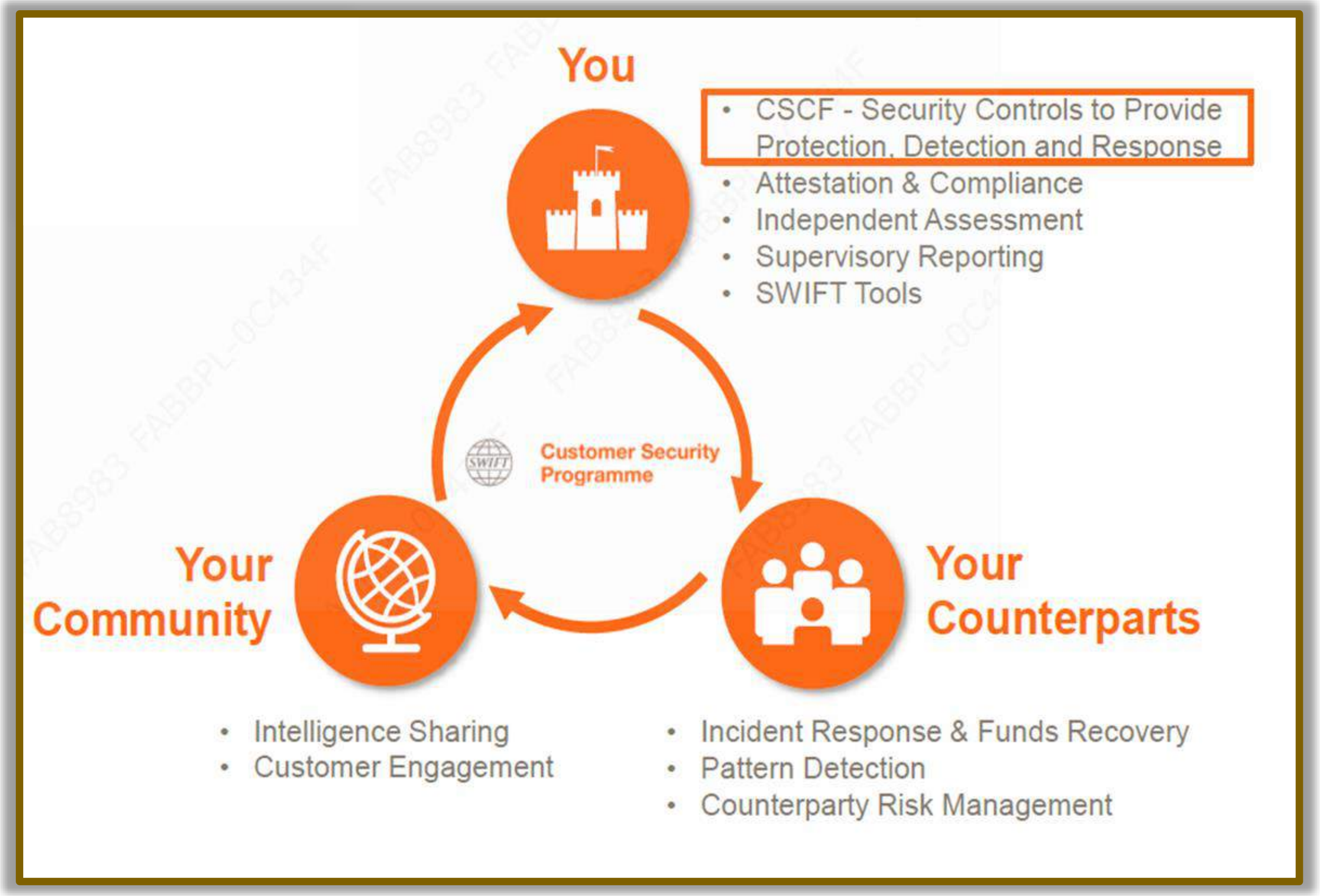
Globex State Bank in Russia $940,000 at risk using system hacking In December 2017, the attackers being able to enter in their bank system. The hackers tried to steal 55 million rubles ($940,000), but were only able to steal $100,000 as the Russian bank detected the suspicious wire transfers.

SWIFT OVERVIEW

Launched in 2016 in response to the sophisticated cyber attacks on SWIFT users, the Customer Security Programme (CSP) seeks to pragmatically 'raise the bar' of cyber-security hygiene across all users, reduce the risk of cyber attacks and minimise the financial impact of fraudulent transactions.

The Customer Security Programme (CSP) was launched in response to the attack on Bangladesh Bank. CSP is a comprehensive multi-year, multi-facetted initiative.

CSP aims to transform the institutional financial services ecosystem by raising the bar of cybersecurity hygiene, reducing the risk of cyberattacks and minimizing the impact of fraudulent transactions.

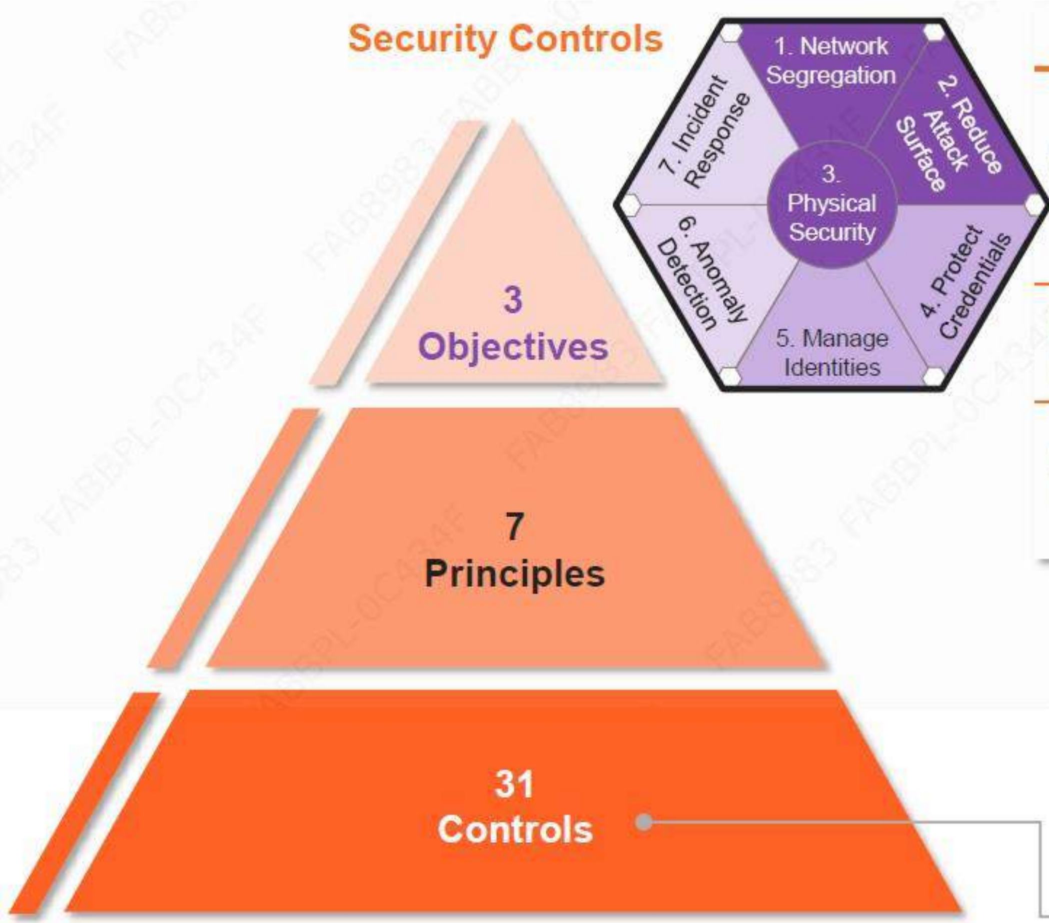


You:
- CSCF - Security Controls to Provide Protection, Detection and Response
- Attestation & Compliance
- Independent Assessment
- Supervisory Reporting
- SWIFT Tools

Your Community:
- Intelligence Sharing
- Customer Engagement

Your Counterparts:
- Incident Response & Funds Recovery
- Pattern Detection
- Counterparty Risk Management

SWIFT OVERVIEW



CSP Security Controls Framework

Secure Your Environment	1.	Restrict Internet access & Segregate critical systems For general IT environment
	2.	Reduce attack surface and vulnerabilities
	3.	Physically secure the environment
Know and Limit Access	4.	Prevent compromise of credentials
	5.	Manage identities and segregate privileges
Detect and Respond	6.	Detect anomalous activity to system or transaction records
	7.	Plan for incident response and information sharing

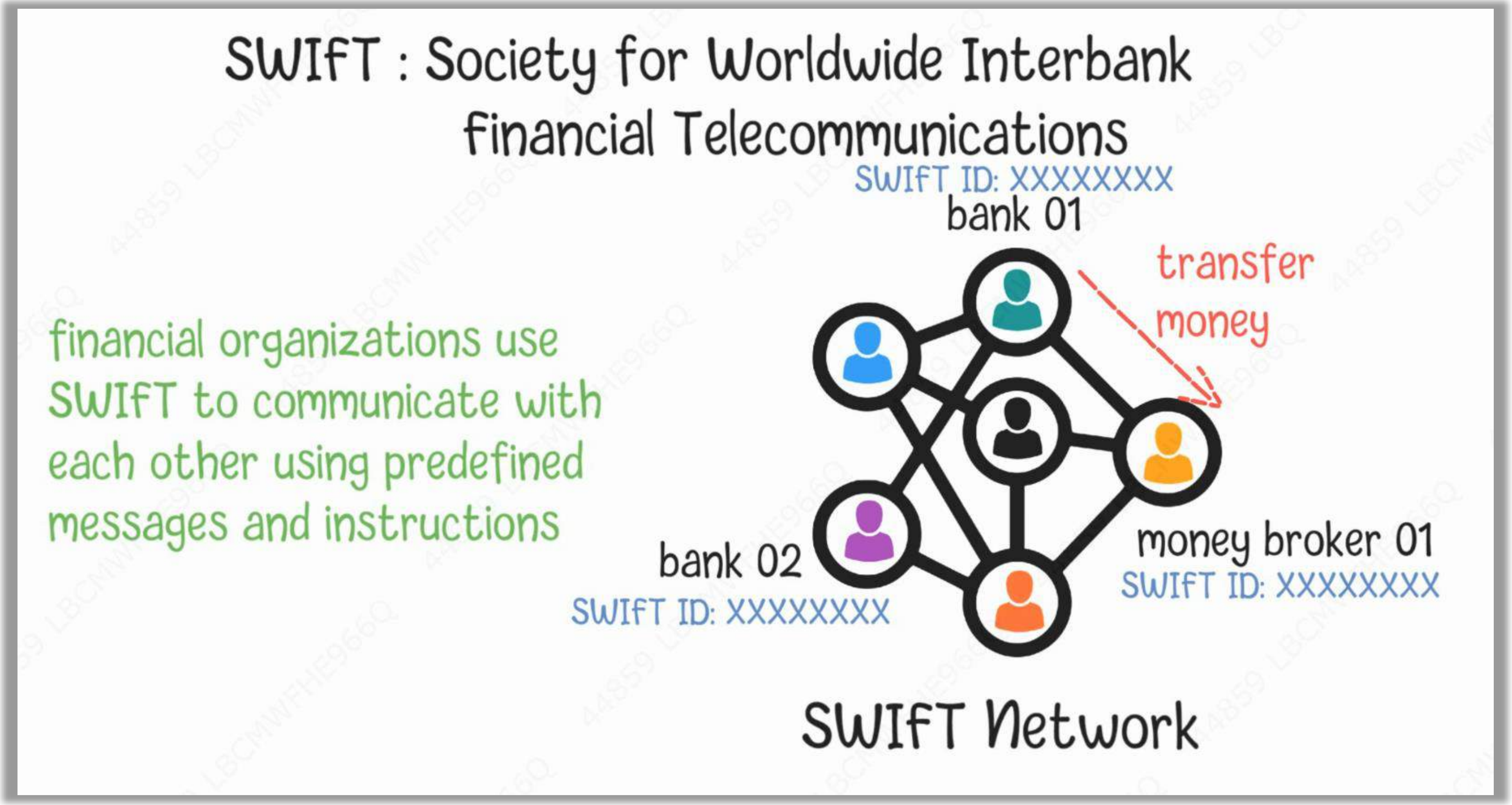
- Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002 (see Appendix E of CSCF)
- 22 controls are mandatory (14 for B Architecture)
- 9 controls are advisory (8 for B Architecture)
- Full compliance against mandatory controls by end 2021

⇒ Integrity and Confidentiality covered as part of Cyber Security

⇒ Availability or Business Continuity Mgt lightly covered

⇒ Scope limited to entry points

How Swift Work



SWIFT : Society for Worldwide Interbank Financial Telecommunications

financial organizations use SWIFT to communicate with each other using predefined messages and instructions

PCI-DSS

Payment Card Industry Data Security Standard

pci

Security Standards Council®

5 BIGGEST CREDIT CARD DATA BREACHES

2019: Capital One (106 Million Customers Exposed)

Capital One, the fifth-largest credit card issuer in the Unites States, revealed in July 2019 that a hacker accessed the personal information of around 106 millioinformationn customers and applicants in the U.S. and Canada. The that was accessed included highly personal details on consumers and small businesses, including names, social security numbers, income and dates of birth as of the time they applied for one of several credit card products from 2005 through early 2019.

2014: The Home Depot (56 Million Cards)

This 2014 attack on the do-it-yourself retailers was perpetrated through a "unique, custom-built malware" according to the Wall Street Journal. Fortune magazine reported that Home Depot (HD) ended up payicustomers. ng $25 million to banks, $134.5 million to card companies like Visa and MasterCard and $19.5 million to affected

2006: TJX Companies (94 Million Cards)

The company that own retailers like TJMaxx and Marshall's (TJX) was a target of a cyber-attack in 2006, reported the Associated Press. While data for both Visa (V) and MasterCard (MA) credit cards was stolen, the AP reported that for Visa alone, the fraud related losses could be to the tune of $68 million to $83 million, spread across 13 countries. Consumer Affairs reported that the company ended up paying $41 million to Visa, $24 million to MasterCard and another $9.75 million in consumer protection settlement to 41 states.

1984: TRW/Sears (90 Million Cards)

Almost 37 years ago, the New York Times reported that the password for a leading credit union TRW was stolen from a Sears (SHLD) store on the West Coast. That password unlocked the credit histories and personal information that could subsequently be used to obtain credit card numbers.

2009: Heartland Systems (160 Million Cards)

A lone hacker broke into the systems of the payment processing company in 2009 and was later caught and jailed. In 2013, five people, including this hacker, were indicted for attacking a number of retailers, financial institutions and payment processing firms and stealing personal identification and credit/debit card data. The total mentioned in that indictment was 160 million cards. Other companies affected included Nasdaq, 7-Eleven, Carrefour, JC Penney, Hannaford, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard.

PCI-DSS Overview

What is PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

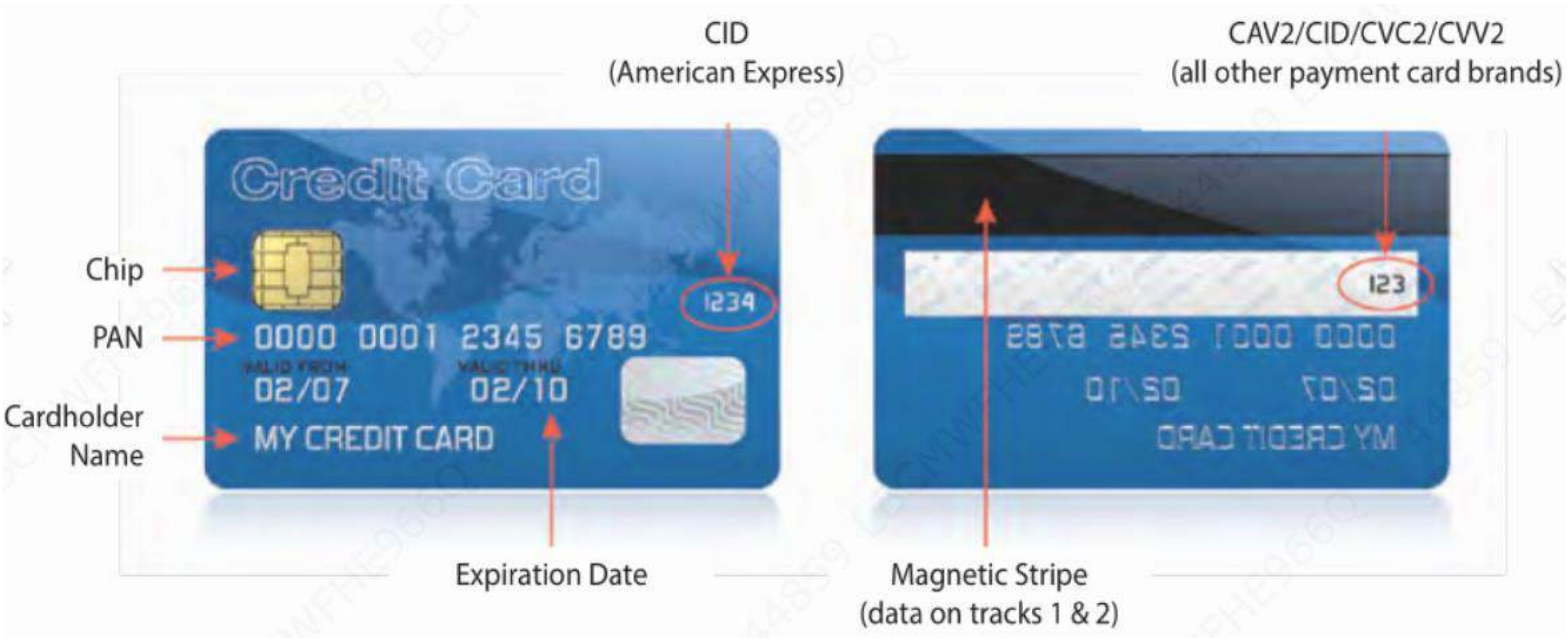
Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

Need for PCI DSS

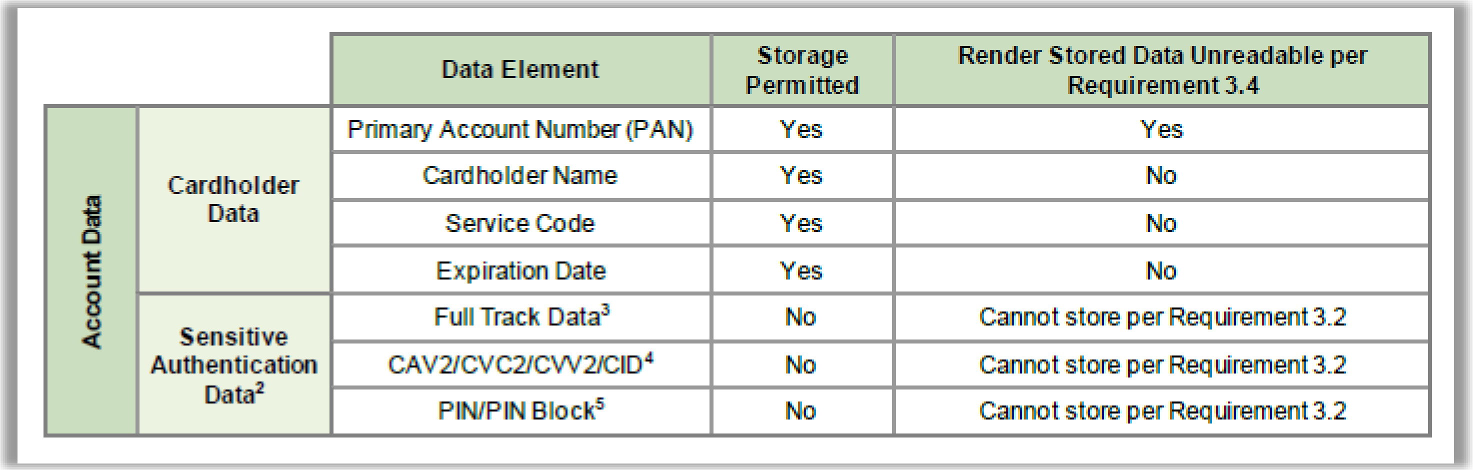
- Enforced by Card Brands and mandated by Central Bank of UAE as a regulatory requirement
- External and Internal reviews to protect card holder data and environment
- Identify and report possible security risks in the existing Process, Business, IT applications and infrastructure on-prem and cloud w.r.t. PCI DSS requirements.
- Conducts Risk Assessment, Firewall & ACL Reviews, VA, Network Segment PT, Internal & External PT, Application PT, Security Policy Review, Card Data Discovery, baselines, Incident Response Test, ODC Review, Third Party Review, Wireless Scanning, User Access Control Review.
- Serves as a layer to provide assurance to the Card Brands, Central Bank, clients, customers.
- Enhance Customer trust and brand reputation
- Enhance bank's security posture

PCI-DSS Overview

Type of Data on a Payment Card



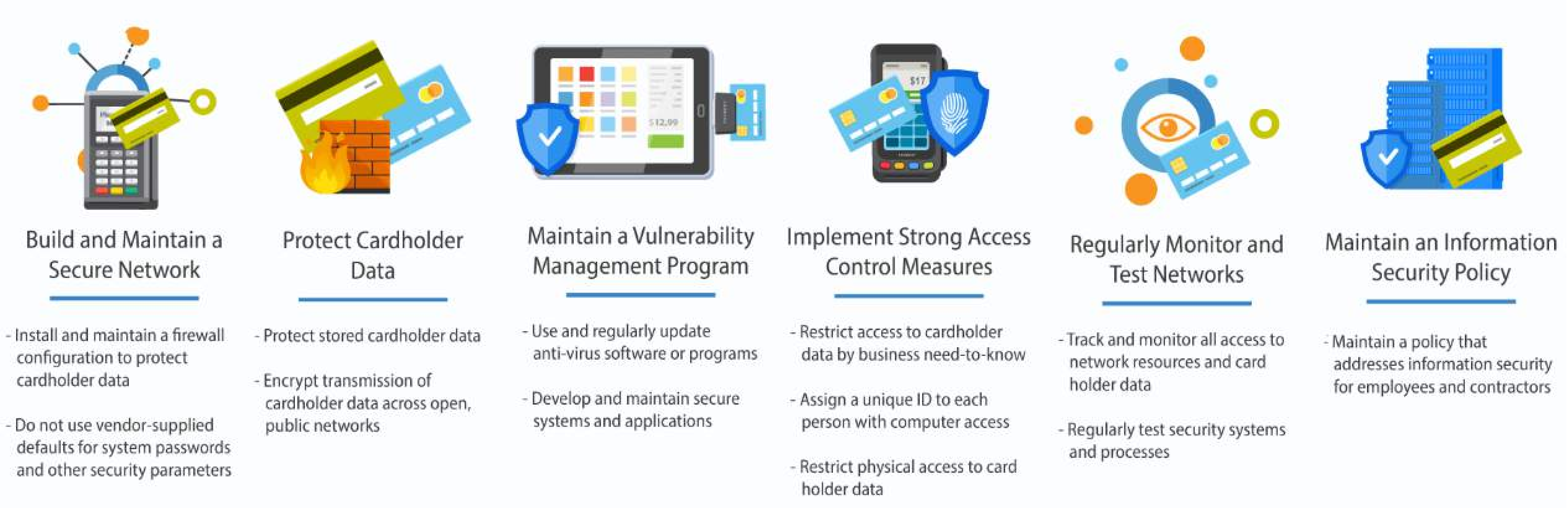
Payment Card Data Classification



		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

PCI-DSS Overview

The PCI DSS consists of a standardized, industry-wide set of requirements and processes for various security controls, ensuring that payment card and cardholder data are protected. There are **6 control objectives**, which are split into 12 requirements (and these are further divided into around 252 sub-requirements)



Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to card holder data

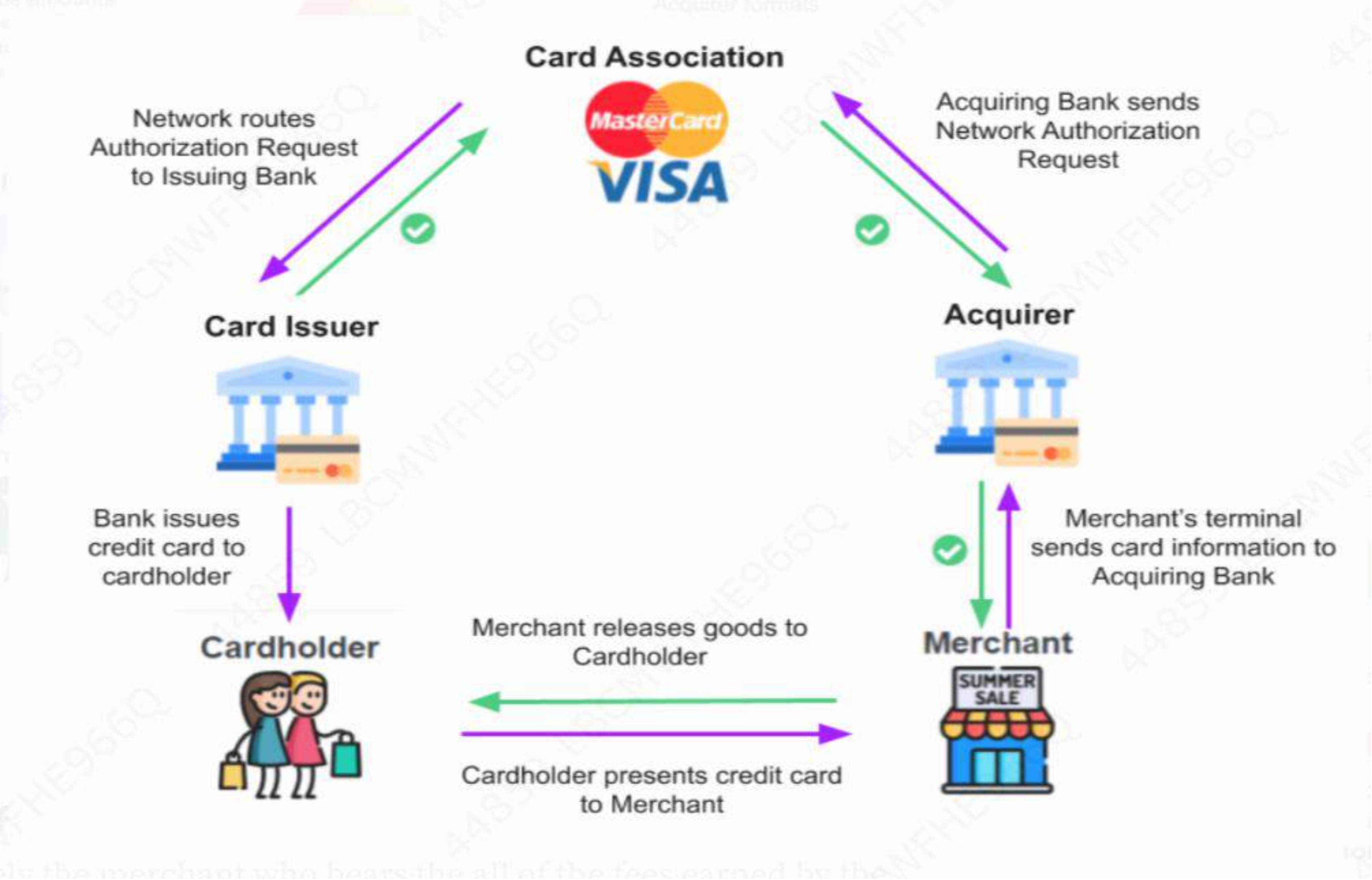
Regularly Monitor and Test Networks

- Track and monitor all access to network resources and card holder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for employees and contractors

Card Authorization Workflow



Network routes Authorization Request to Issuing Bank

Acquiring Bank sends Network Authorization Request

Bank issues credit card to cardholder

Merchant's terminal sends card information to Acquiring Bank

Merchant releases goods to Cardholder

Cardholder presents credit card to Merchant

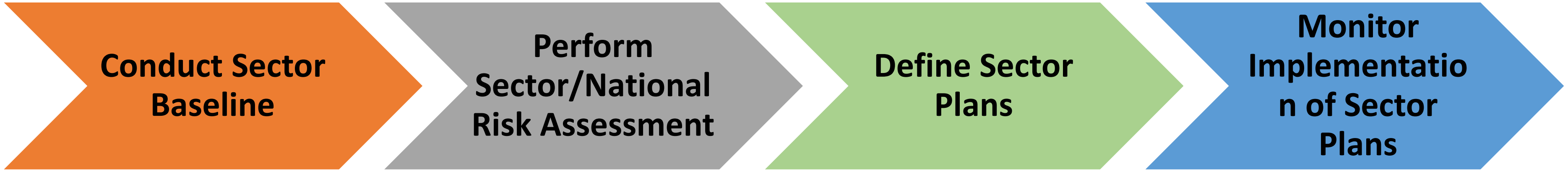
NESA

الهيئـــة الوطنيـــة للأمـــن الإلكتـرونـــي
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربيـة المتحـدة

NESA UAE IA OVERVIEW

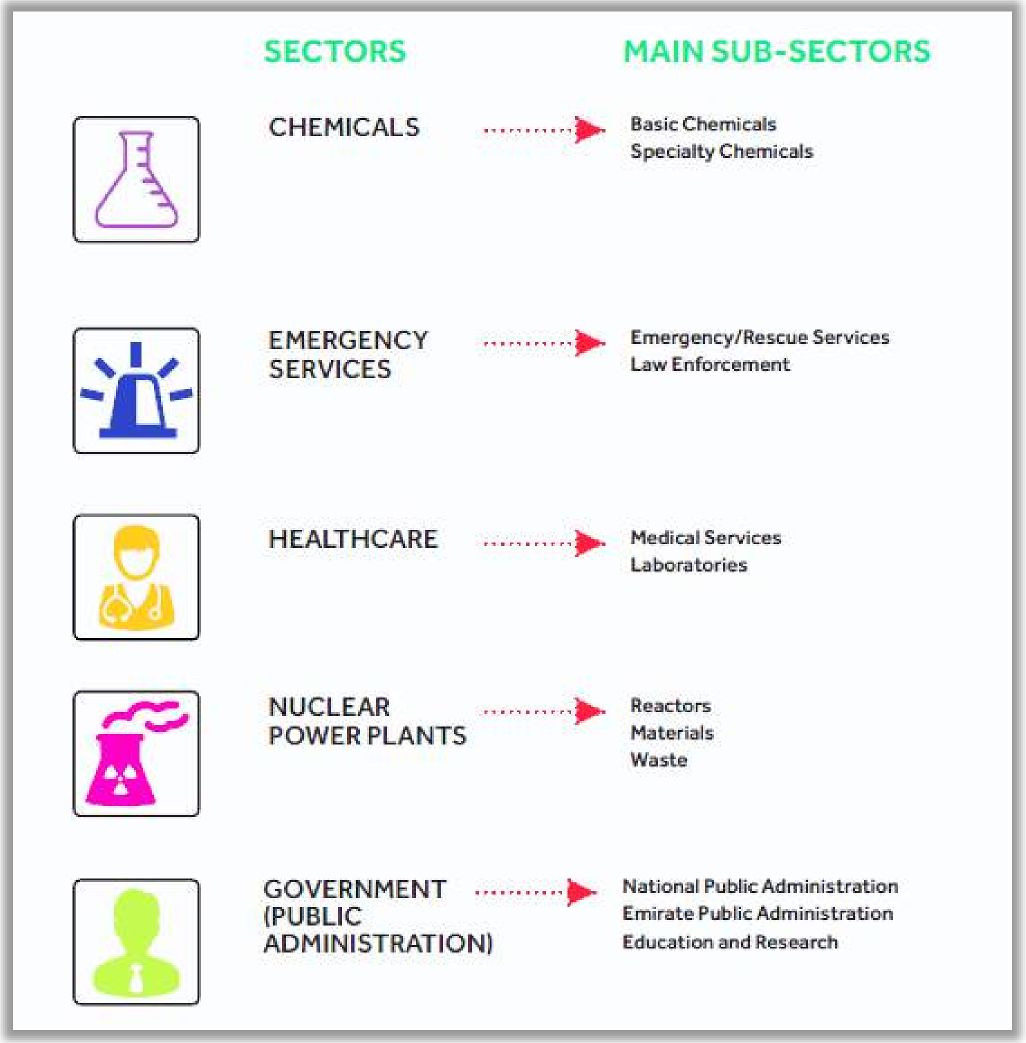
The purpose of the UAE IA Regulation is to provide requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the UAE

Objectives	Building a unified, competitive and resilient economy across all emirates.
	Support other initiatives involving national security, economic development and the improvement of daily life for UAE citizens and residents.

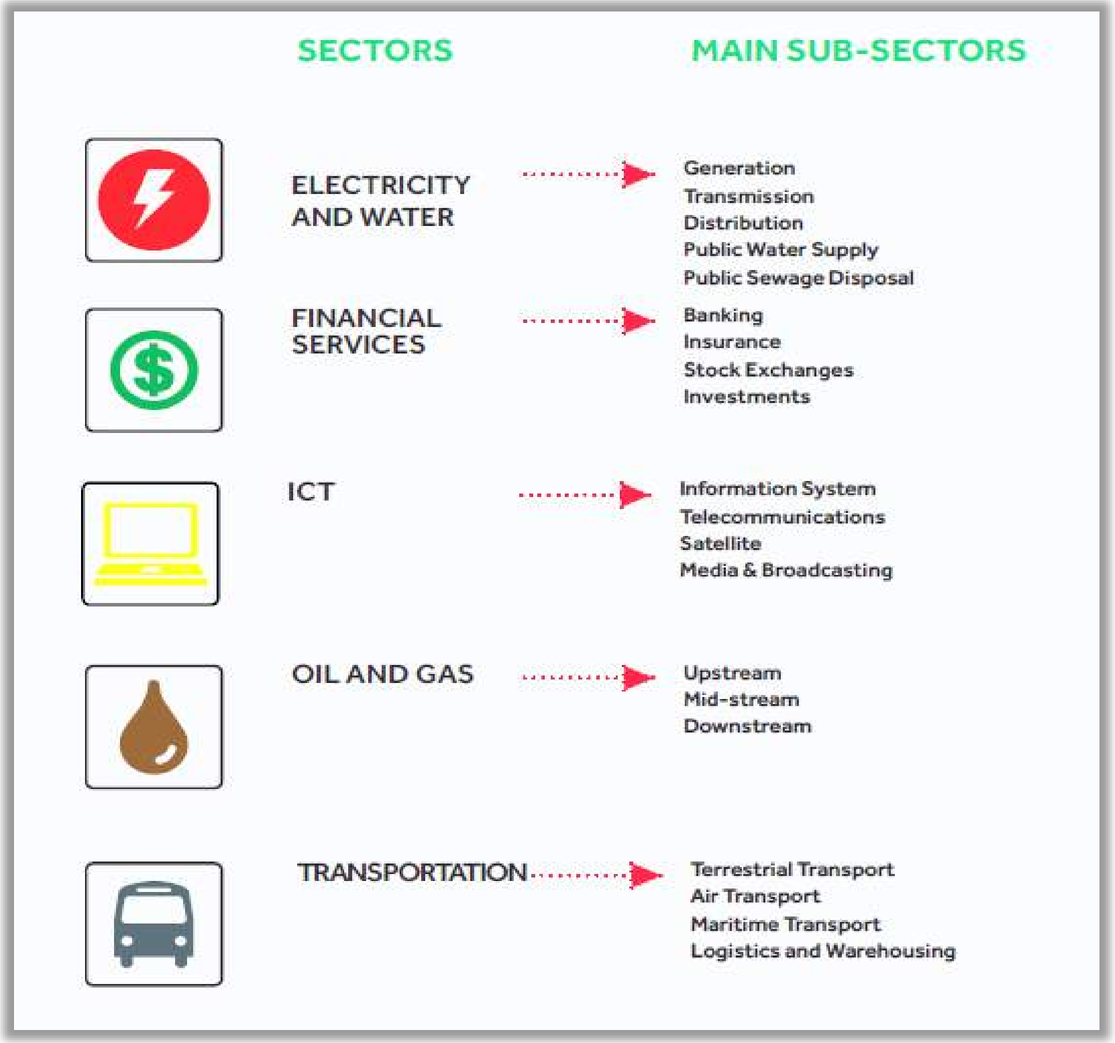


Phase	**Conduct Sector Baseline**	**Perform Sector/National Risk Assessment**	**Define Sector Plans**	**Monitor Implementation of Sector Plans**
Key Activities	• Prioritize sectors for CIIP program implementation • Engage with sector operators and regulators to establish joint activities • Identify critical national services for risk assessment	• Identify information infrastructures supporting critical national service • Assess threats and vulnerabilities to develop Operator CII Risk Assessment • Consolidate the Sector CII Risk Assessments to create the National CII Risk Assessment	• Identify CII Cyber Security requirements that will reduce the identified risks • Define Sector Plans to meet the CII Cyber Security requirements	• Implement Sector Plans • Monitor the Sector Plan implementation to ensure requirements are met

NESA UAE OVERVIEW: SCOPED SECTORS



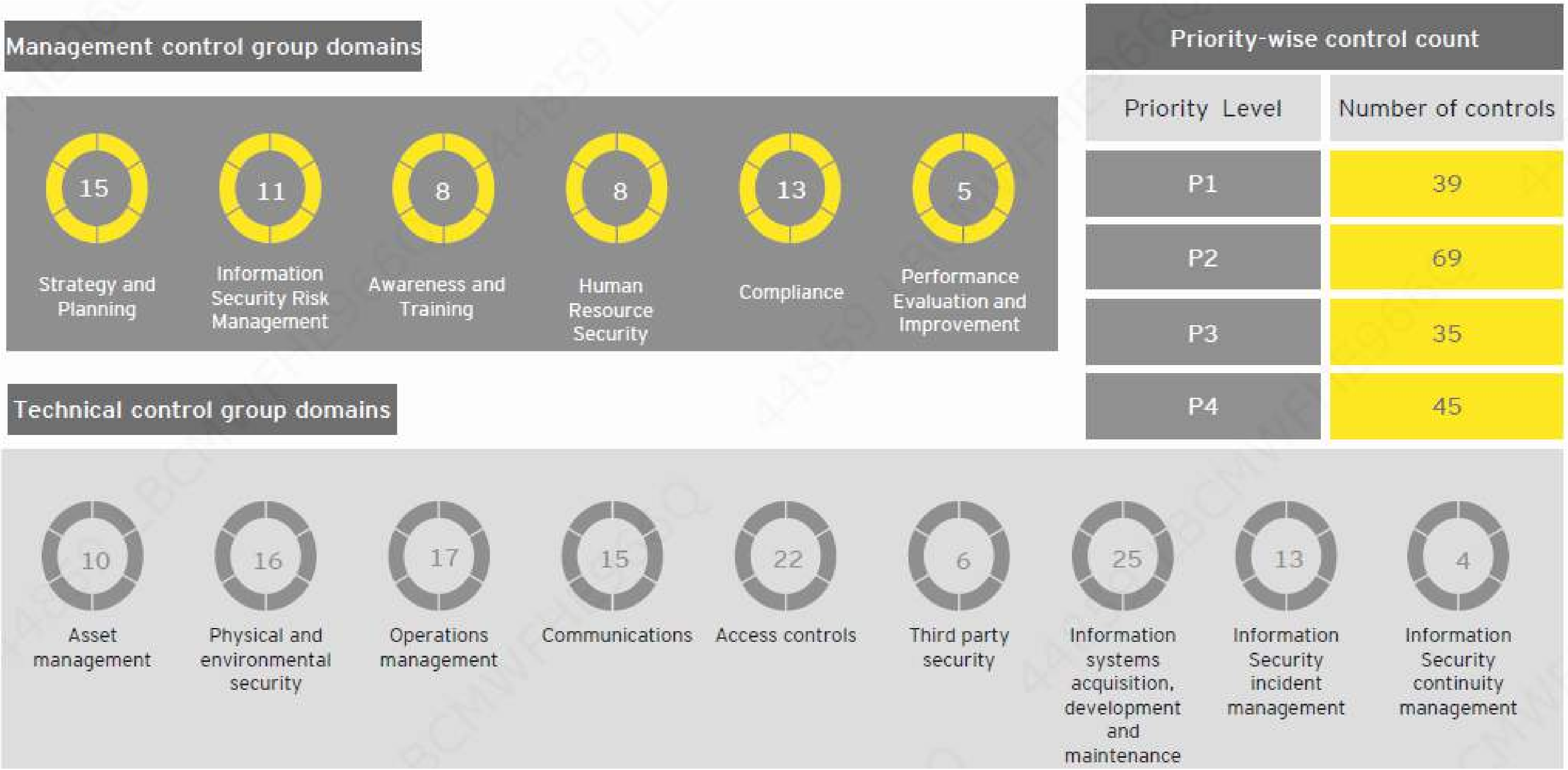
SECTORS	MAIN SUB-SECTORS
CHEMICALS	Basic Chemicals Specialty Chemicals
EMERGENCY SERVICES	Emergency/Rescue Services Law Enforcement
HEALTHCARE	Medical Services Laboratories
NUCLEAR POWER PLANTS	Reactors Materials Waste
GOVERNMENT (PUBLIC ADMINISTRATION)	National Public Administration Emirate Public Administration Education and Research



SECTORS	MAIN SUB-SECTORS
ELECTRICITY AND WATER	Generation Transmission Distribution Public Water Supply Public Sewage Disposal
FINANCIAL SERVICES	Banking Insurance Stock Exchanges Investments
ICT	Information System Telecommunications Satellite Media & Broadcasting
OIL AND GAS	Upstream Mid-stream Downstream
TRANSPORTATION	Terrestrial Transport Air Transport Maritime Transport Logistics and Warehousing

NESA UAE Overview

The NESA IAS comprises of 60 management and 128 technical controls.
Under the 188 controls NESA IAS defines 135 mandatory sub controls and 563 sub controls based on risk assessment with priorities assigned to each control



Management control group domains

15	Strategy and Planning
11	Information Security Risk Management
8	Awareness and Training
8	Human Resource Security
13	Compliance
5	Performance Evaluation and Improvement

Technical control group domains

10	Asset management
16	Physical and environmental security
17	Operations management
15	Communications
22	Access controls
6	Third party security
25	Information systems acquisition, development and maintenance
13	Information Security incident management
4	Information Security continuity management

Priority-wise control count

Priority Level	Number of controls
P1	39
P2	69
P3	35
P4	45

Based on the circular released on **10th September 2018** by the Central Bank of the United Arab Emirates (UAE).
All the banks in the UAE are required to comply with the NESA IAS, by adopting the best security standards and leading information security practices.

Classified: Internal\ FAB Internal

Thank you