



IDC CISO Summit 2019

Risky Business: Understanding Digital Risk to Ensure Digital Trust

Protecting the Crown Jewels: SWIFT Infrastructure

Semih GELİŞLİ

IT Security Incident Management Unit
Manager

Yapi ve Kredi Bankası

Who am I?

Yıldız Technical University – Computer Engineering

Bahçeşehir University – Managed Information Systems

Doğan Gazetecilik – IT Security Specialist (2,5 Year)

Garanti Teknoloji – Network Security Platform Specialist (~3 Year)

Yapi ve Kredi Bankası – IT Security Incident Management Specialist (~2.5 Year)

Agenda

What is SWIFT?



Detection &
Prevention
Controls



Significant Cyber
Incidents



Lessons Learned

Crown Jewels



What is SWIFT?

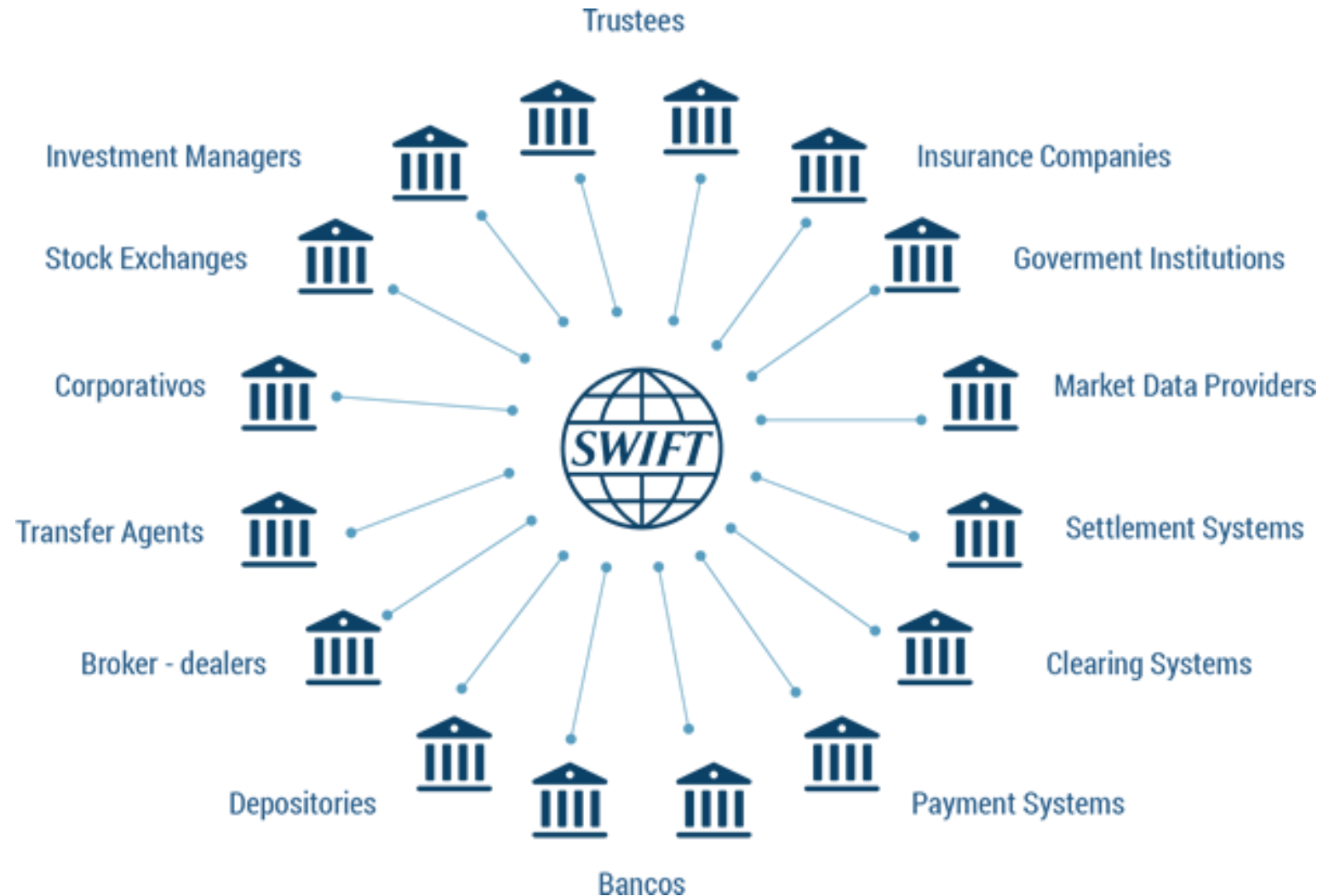
SWIFT stands for the **Society for Worldwide Interbank Financial Telecommunication**.

SWIFT Community:

200+ Country

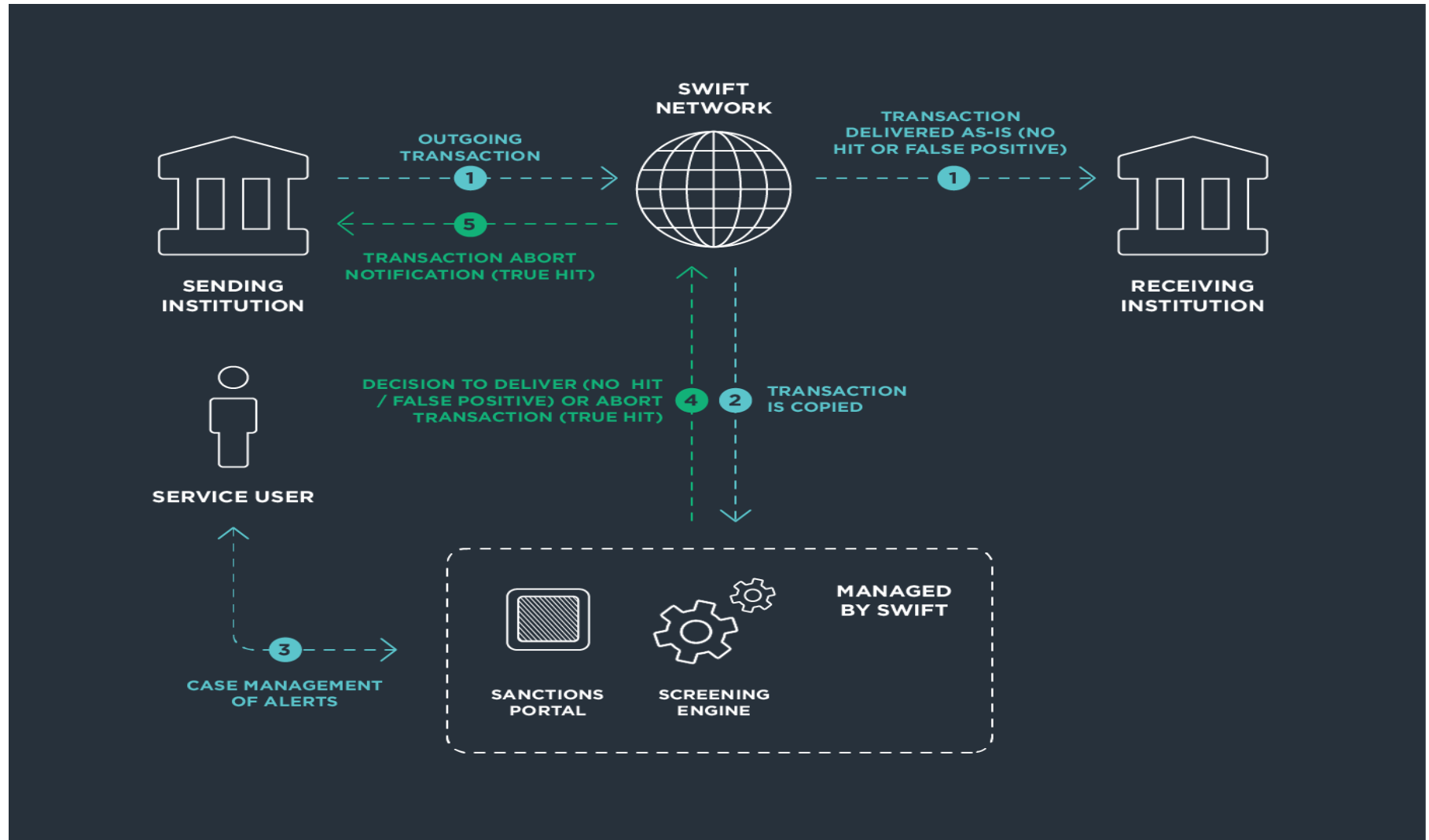
10.000+ Correspondents

More than \$100 billion are being send daily.



How SWIFT Works?

SWIFT **transports** financial messages in a **highly secure** way; but it is not financial institution. It does not hold accounts for its members.



Agenda

What is SWIFT?



Detection &
Prevention
Controls



Significant Cyber
Incidents



Lessons Learned

Significant Cyber Incidents

Advanced Persistent Threat Groups

Most known **APT Groups** that
targets Financial Institutes & Turkey

Cobalt Gang
Lazarus
SILENCE
APT38
Muddy Water
...



Significant Cyber Incidents

Bangladesh Bank Case

Over the weekend of 5th February 2016, hackers attempted to steal **\$951 million** from the **Bangladesh Central Bank** (BCB) in Dhaka. Much of this was eventually recovered, but the thieves still managed to get away with **\$81 million**.

Hackers **misspelled** “foundation” in the NGO’s name as “fandation”, prompting a routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which **stopped the transaction**, one of the officials said.



Significant Cyber Incidents

Bancomext Case

Cyber criminals who are believed to be affiliated with **North Korea** managed to infiltrate **Bancomext**.

Their plan to steal **\$110 million** was foiled by a vigilant bank employee who managed to stop the transfer before it arrived at its destination (they were disguised as donations from the Mexican bank to a Korean church. **Fortunately** when the fraudulent transaction was requested, banks in Korea were closed, and Bancomext managed to **reverse** the transaction before they opened).



Significant Cyber Incidents

Banco De Chile Case

Banco de Chile loses \$10 million and 9,000 hard drives in hack.

The bank started **cancelling** these transactions, but not all of them were recovered.

The bank released a statement that said, translated, that desktop PCs across **offices, terminals** and **computers across branches**, and the phone service had been **affected by the virus**. Reports indicate the **virus wiped hard drives** and left them **unusable**.



Significant Cyber Incidents

Bank of Valletta Case

Hackers tried to steal **€13 million** from Malta's **Bank of Valletta**.

Bank of Valletta (BOV) employees discovered the hackers' intrusion during Daily reconciliation operations of international transfers.

Roughly 30 minutes after finding the **unauthorized operations**, the bank closed all its branches, **shut down** its **ATM** and **point-of-sale systems**, along with its **website** and **e-banking servers**.



Agenda

What is SWIFT?



Detection &
Prevention
Controls



Significant Cyber
Incidents



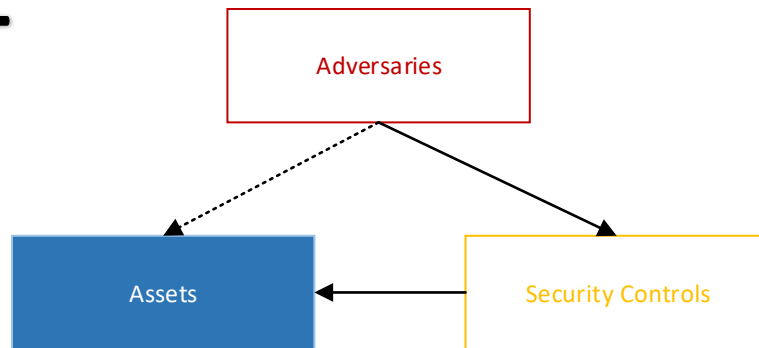
Lessons Learned

Detection & Prevention Controls

Risk-Based Defense

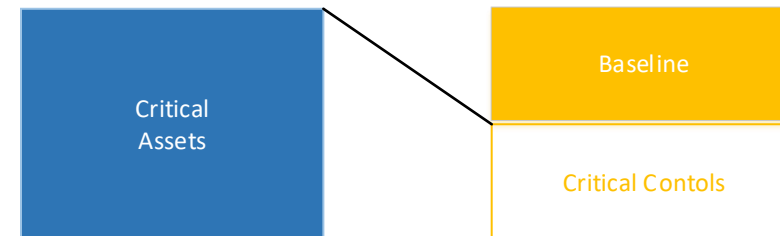
1

Understand Your Controls



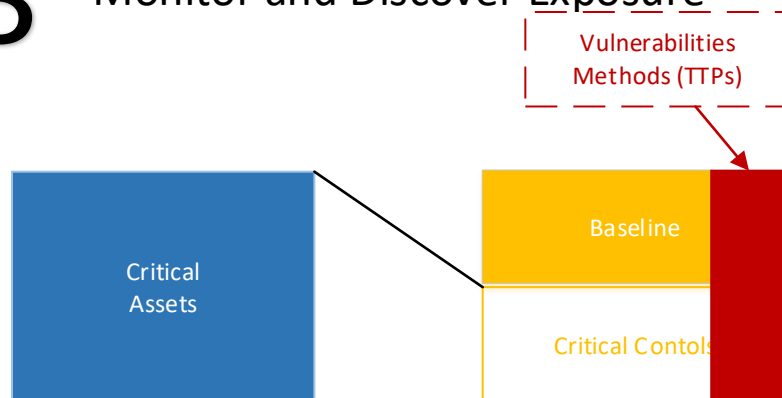
2

Critical Controls for Your Critical Assets



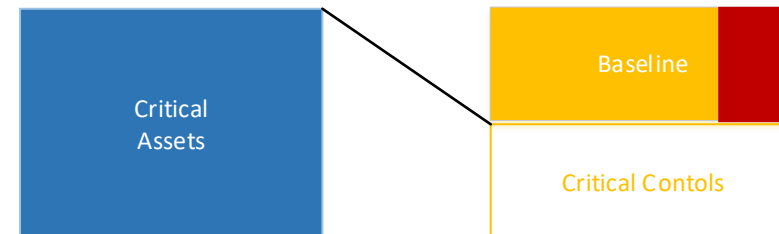
3

Monitor and Discover Exposure



4

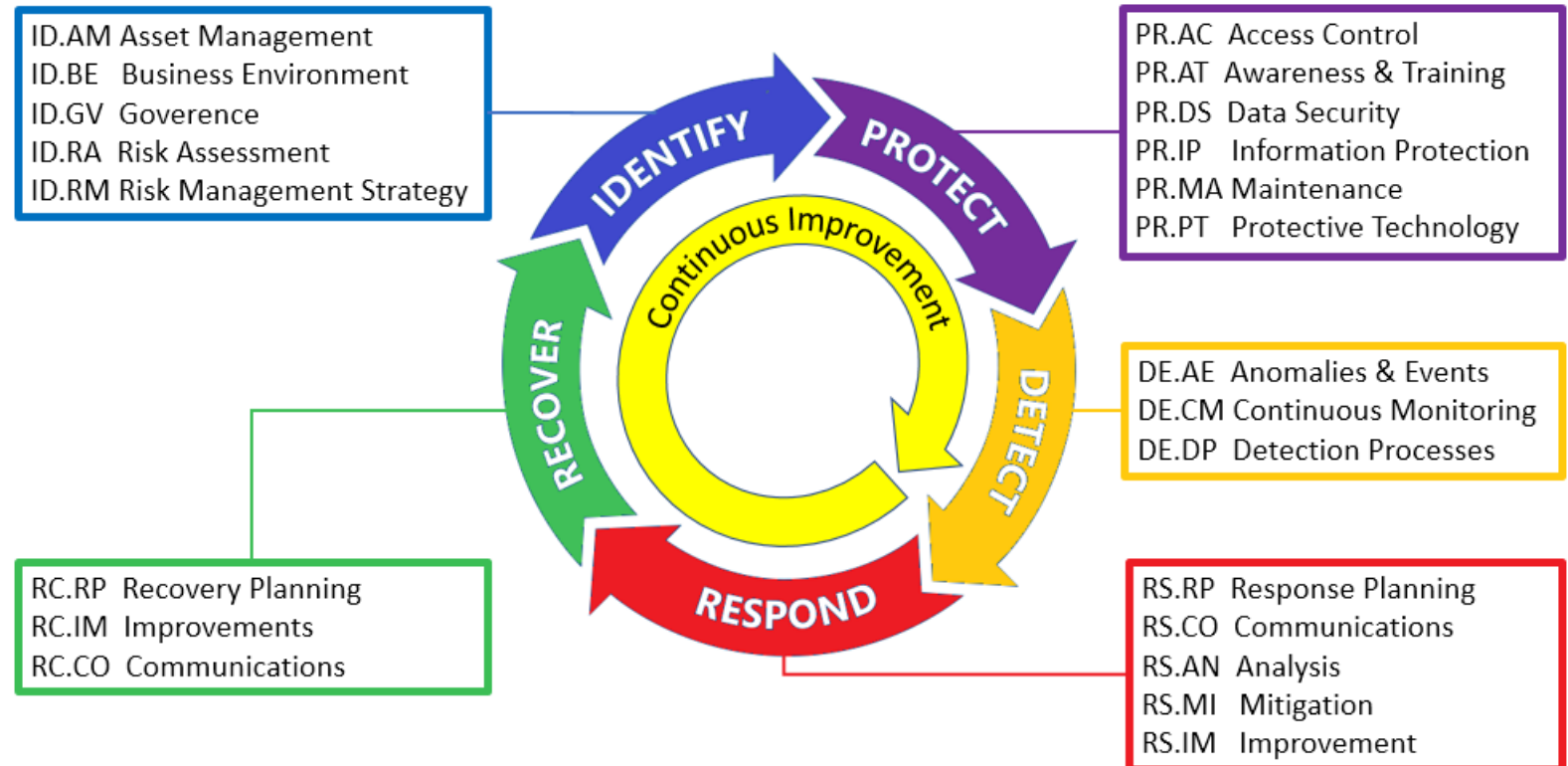
Adapt Your Controls



Detection & Prevention Controls

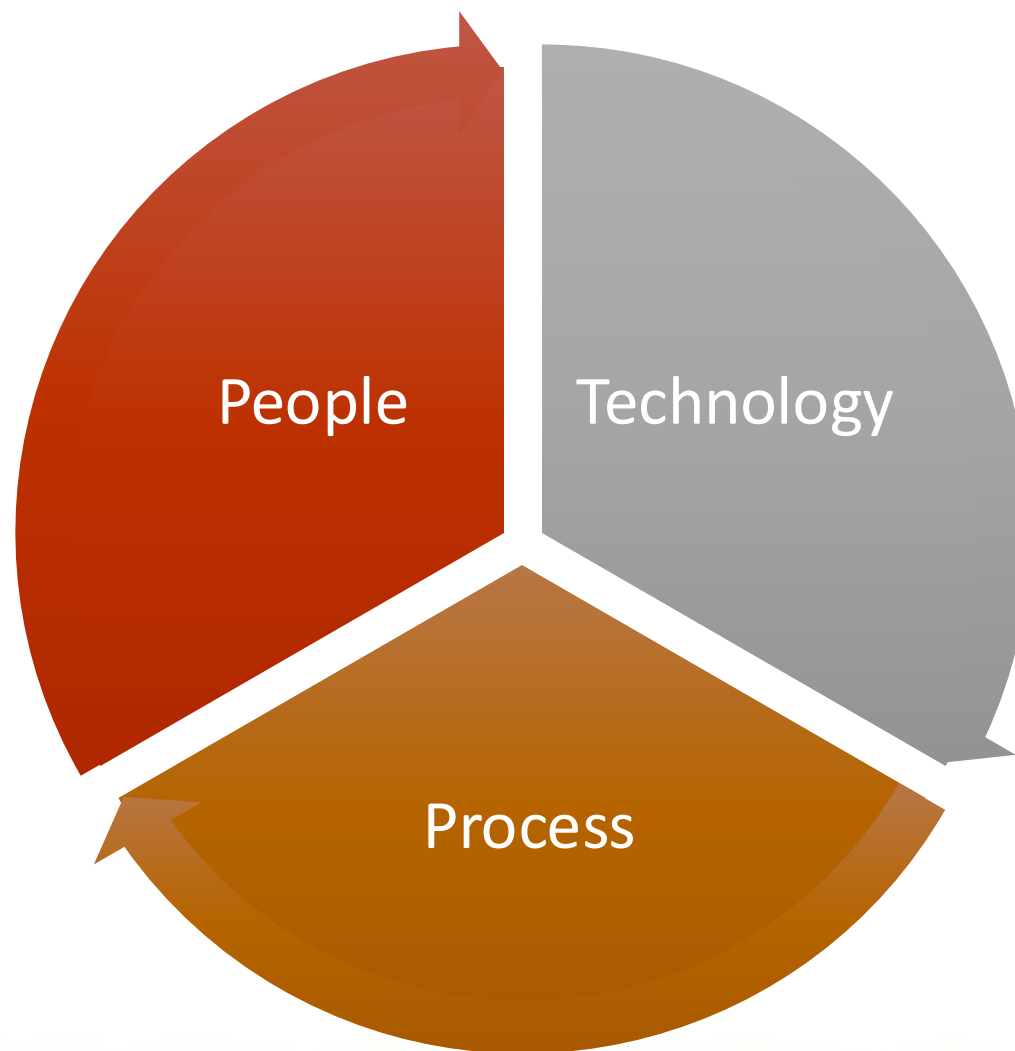
Compliance & Best Practices

- SWIFT Customer Security Programme
- CIS (Center for Internet Security) Controls
- NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- ISO 27001
- PCI DSS
- ACSC (Australian Cyber Security Center) Malicious Email Mitigation Strategies
- BDDK Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Yönetmeliği









Detection & Prevention Controls

People Process Technology



Detection & Prevention Controls

Gain Visibility

Log sources	Advanced Persistent Threat 	Insider Threat 	Securing the Cloud 	Critical Data Protection 	Incident Response 	Compliance 	Risk and Vulnerability Management 
Firewall/Router	✓		✓	✓	✓	✓	✓
IDS/IPS (Intrusion Detection System/Intrusion Protection System)	✓			✓	✓		✓
Web Proxy	✓	✓	✓	✓		✓	
VPN	✓						
DNS	✓	✓					✓
DHCP	✓	✓			✓		
Mail Logs	✓	✓		✓			
DLP (Data Loss Prevention)	✓	✓		✓		✓	
Endpoint	✓	✓		✓		✓	✓
Identity/Authentication (LDAP/AD/Radius)	✓	✓	✓		✓		
Anti Virus	✓			✓	✓	✓	✓

Detection & Prevention Controls Assessment

- ❖ Cyber Security Risk Assessments
- ❖ Red Teaming
- ❖ Compromise Assessment
- ❖ Table Top Exercises

Agenda

What is Swift?



Detection &
Prevention
Controls



Significant Cyber
Incidents



Lessons Learned

Lessons Learned

Apply – Do This

- Next week you should:
 - ❖ Know your crown jewels
 - ❖ What is your value as a company?
 - ❖ What can be your greatest risks?
 - ❖ Who can be your attackers? (Nation states, Script kiddies, etc.)
 - ❖ What can be their motives? (Profits, disrupt, etc.)
- In the first three months following this presentation you should
 - ❖ Identify Your Adversaries
 - ❖ Identify and deploy at least three use cases in your organization
- Within six months you should
 - ❖ Implement Security Awareness Program
 - ❖ Follow a Security Framework

Questions

