

Telenor Group Internal Audit and Investigation

Creating business value through independent fact-based assessments



Ahmad Wajid

Vice President – IT & Cybersecurity Audits, Telenor

- Working in Internal Audit for Telenor for almost 10 years
- London School of Economics graduate in Management and Information Systems
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Ethical Hacker (CEH)
- Six Sigma Yellow Belt
- Gamer dad with 2 kids



My teams skillset includes:

1. IT Governance, Control and Third Party Management specialists
2. Hands-on Cyber Security specialists
3. Telecom-Engineering specialists

- 1. About Telenor & Telenor Group Internal Audit and Investigation**
- 2. A Glimpse of our 3 year IT audit plan and process**
- 3. Some reflections on Business Continuity Planning audits**
- 4. Some reflections on Cyber Security audits**
- 5. Questions ?**

About my Company – Telenor ...



- A leading telecommunications company with **186 million** customers and annual sales of around **USD 12 billion (2019)**.
- Holds #1 or #2 positions in most of our markets. Listed at Oslo Stock Exchange.
- Has mobile operations in the Nordics, including Norway, Sweden, Denmark and Finland. In Asia, Pakistan, Bangladesh, Myanmar, Thailand and Malaysia.



About Telenor Group Internal Audit & Investigations ...


Group Internal Audit and Investigation
Tone Skuterud SVP (FBU)



Strategy, methodology & planning (1)
Per Pundsnes (FBU)



Investigation (8)
Paul Doran (FBU)



- Integrity Hotline
- Reported concerns
- Internal investigations

Specialists from listed subsidiaries


IT and cyber security (4)
Ahmad Wajid (Pakistan)



- IT, Network and Cyber security
- IT governance audits
- Investigation support

Specialists from listed subsidiaries

Governance & Third parties (3)
Maris Valts (FBU)



- Governance related audits
- Third-party audits
- Shared services & sourcing

Specialists from listed subsidiaries


Core business and Digital (9)
Jean Sebastien Scmitt (FBU)



- Core telecom
- Digital business
- Data mining and forensic

Specialists from listed subsidiaries


Financial Services (2)
Alex Zefri (Singapore)



- Financial Services audits
- Microfinance
- Digital banking

Local FS teams as required by law

Localized teams (5)
Amna Tahir (Pakistan)



- Planning
- Follow-up
- Reporting

Listed Businesses



Anushia
Hasan Faisal
Kiti

A Glimpse of our 3 year IT Audit Plan

2019 Themes

Review Program 1: IT Governance in Telenor

- a. Strategic Governance
- b. **Business Continuity & Disaster Recovery**

Review Program 2: Effectiveness of Business Security:

- a. Business Security Strategy
- b. Global Security Operating Model
- c. Defendable Architecture
- d. Physical Security of key sites

Third Party Management Audits (IT and Telco):

- a. CDC IT in TM (Wipro)
- b. CDC Network in TP (Nokia)
- c. CDC Network in Digi (Ericson)
- d. Telco Network in Telenor Norway (Huawei)

2020 Themes

Telco areas

1. Network Net Promoter Score (NPS)
2. Network Preventive Maintenance, End of life, and Replacement
3. Network Energy Management
4. Telecom Network Security Governance & SS7 Vulnerability Management.
5. Tools & Capability uplift through Network CDC Project
6. Third Party management (program continuing) including Ericsson (Dtac) & Nokia (Norway)

IT areas

1. Public Cloud Applications - Management and Security
2. Data Lake Management & Business Intelligence
3. Customer data in critical systems and processes - Identity and Access management
4. **Basic Cyber Security hygiene**

2021 Themes

Telco areas

1. Network Complaint Handling
2. Telecom Regulatory Compliance
3. Site Planning & Deployment
4. Network Performance Management
5. Third Party Management Audits continued
6. Physical Security (Follow-up from 2019)

IT areas

1. IT Migration in the Telenor Hybrid Cloud
2. Automation and Simplification in Telenor
3. Security & Privacy Considerations within Contracts
4. Cyber Security Awareness routines
5. **Basic Cyber Security hygiene continued**

emergency infrastructure GOVERNMENT
infrastructure emergency
CRITICAL emergency
infrastructure emergency
DISASTER
business
recovery
training
resilience
PLAN
safe
protection
education
risk
disaster
operations
CONCEPT COOP
OPERATIONS safe



Possible Disaster Scenarios for a Company like Telenor

Possible Scenarios:

- **Cyber Security Breach**
- **Operational mistakes in IT**
- **Critical system crash**
- **Fire**
- **Sabotage**
- **Flood**
- **War**
- **Curfew/Governmental restrictions**
- **Sanctions (including on a critical outsourcing partner)**
- **Employees strike**
- **Suicide attacks.**
- **Critical Site collapsed/sealed.**
- **Force Majeure**

Severe Consequences

- **Financial**
- **Reputational**
- **Opportunity Loss**





But there is plenty of good guidance out there:

- **BSI 25999:2007**
- **ISO-IEC 20000**
- **ISO/IEC 27002**
- **ITIL**
- **GTAG**
- **COBIT**

Summary of our audit program on BCP

1. Have you defined business continuity scope?

- a) Identify critical business processes (internal & outsourced)
- b) Identify essential support processes and IT services
- c) Define a scope (be focused).

2. Have you evaluated business continuity management options and chosen a cost-effective and viable continuity strategy?

- a) Identify potential disruption scenarios
- b) Understand the possible impact on processes and business
- c) Estimate the time required for recovery and determine if its acceptable?
- d) Identify possible business \ technical options and associated costs.
- e) Endorse strategic approvals for selected options.

3. Have you developed and implemented a BCP?

- a) Define roles and responsibilities and resources needed for response and communication.
- b) Maintain operational run-books to enable full or temporary recovery. Ensure links to vendors if needed.
- c) Information Integrity checks once recovery is done?
- d) Define Back-up arrangements needed to support recovery.

4. Are you testing your BCP?

- a) Schedule and test the BCP
- b) Analyse and Update

Summary of our audit program on BCP - continued



5. Are you reviewing maintaining and improving your continuity plans?

- a) **New systems? Process changes?**
- b) **Review and improve.**

6. Are you conducting continuity plan training?

7. Are you managing your back-up arrangements well enough?

- a) **Back-up type and schedule**
- b) **Onsite or Offsite?**
- c) **Periodically test back-ups**

8. Are you conducting post-resumption reviews?

- a) **Assess adherence to the BCP**
- b) **Improve**

Cyber Security

```

PUBLIC BUTTON CRE
RETURN NEW WINDO

PUBLIC CLASS OAFAC
OVERRIDE
PUBLIC BUTTON CRE
RETURN NEW BUTTO

PUBLIC CLASS WINBUT
OVERRIDE
PUBLIC VOID PAINT
SYSTEM.GET.PRINTI

PUBLIC CLASS OMBUT
OVERRIDE
PUBLIC VOID PAINT
SYSTEM.GET.PRINTC

PUBLIC CLASS MAIN
PUBLIC STATIC VOID MAIN
GUIFACTORY FACTO
FINAL STRING APPEA
IF (APPEARANCE ARR
FACTORY = NEW COLE
ELSE IF (APPEARANCE
FACTORY = NEW WIND
ELSE
THROW NEW EXCEPTI

PUBLIC BUTTON BUTT
BUTTON PAINT()

THIS IS JUST FOR THE
WITH ABSTRACT FACTO
@RETURN

PUBLIC STATIC STRING
FINAL STRING() APPEA
APPEARANCEARRA

```

Cyber threat actors

Motivation, resources and capabilities

Nation states and contractors

- Foreign government espionage
- Commercial espionage
- Sabotage and cyberwarfare

Organized crime & targeted attacks

- CEO fraud
- Identity and credit card theft
- Extortion

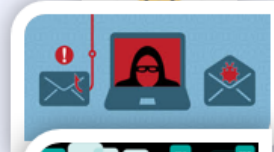
Opportunistic crime and hacktivism

- Website defacement
- Ransomware
- Computer viruses, worms and trojans

Exploiting basic human psychology are common attack vectors



An estimated 52% of attack occur due to human error



Spear-phishing is one of the most prevalent methods of conducting a targeted cyber attack



A recent Verizon report suggests that senior executives are 12 times more likely to be the target of cyber attack



However, attackers are increasingly turning to exploiting employees knowing they have access to sensitive information too

How IA can make cyber manageable for Top Management

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

Some considerations:

1. Take a step by step approach.
2. Focus on fixing the basics
3. Build a foundation for future audits.

Any Questions?



shutterstock.com • 1054528985