etis | THE COMMUNITY FOR TELECOM PROFESSIONALS

The ET-ISAC Telco Security Landscape 2024

Rolv R. Hauge
BCM Manager, Telenor Norway
Chairman, ETIS Information Security WG

ABOUT ETIS

Founded 1991
30 telco Partners and 17 supporting parties,
from 21 European countries,
collaborating in 18 working groups

MISSION

to provide our community with a highly trusted collaboration platform within the European telecommunication industry

OUR ACTIVITIES

100+

Yearly Online Activities

Webinars

Workshops

Roundtables

30+

Yearly Physical Activities

ETIS Annual Gathering

Working Group meetings

TANGIBLE

Outcomes

Surveys

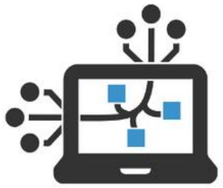
Benchmarks

Position papers

OUR WORKING GROUPS AND TASK FORCES

DIGITAL TELCO STRATEGY FORUM

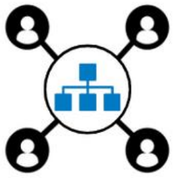
ENERGY REDUCTION TASK FORCE



NETWORK + IT TRANSFORMATION WG

CLOUD WG

BUSINESS CONTINUITY TASK FORCE



ENTERPRISE ARCHITECTURE TASK FORCE

TV CONTENT TASK FORCE

INFORMATION SECURITY WG

SECURITY AWARENESS TASK FORCE

CERT-SOC TELCO NETWORK

ANTI-ABUSE TELCO NETWORK

DATA PRIVACY TASK FORCE

DIGITAL SALES + CUSTOMER EXPERIENCE WG

DIRECT CARRIER BILLING WG

SMART CHARGING + PAYMENTS WG

SUSTAINABILITY WG

CSRD COMPLIANCE TF

PROCUREMENT + SUPPLY CHAIN MANAGEMENT WG

2022: The ET-ISAC is formed

Empowering EU-ISACs

etis | THE COMMUNITY FOR TELECOM PROFESSIONALS

INFORMATION SECURITY WG + CERT-SOC TELCO NETWORK = **ET-ISAC**

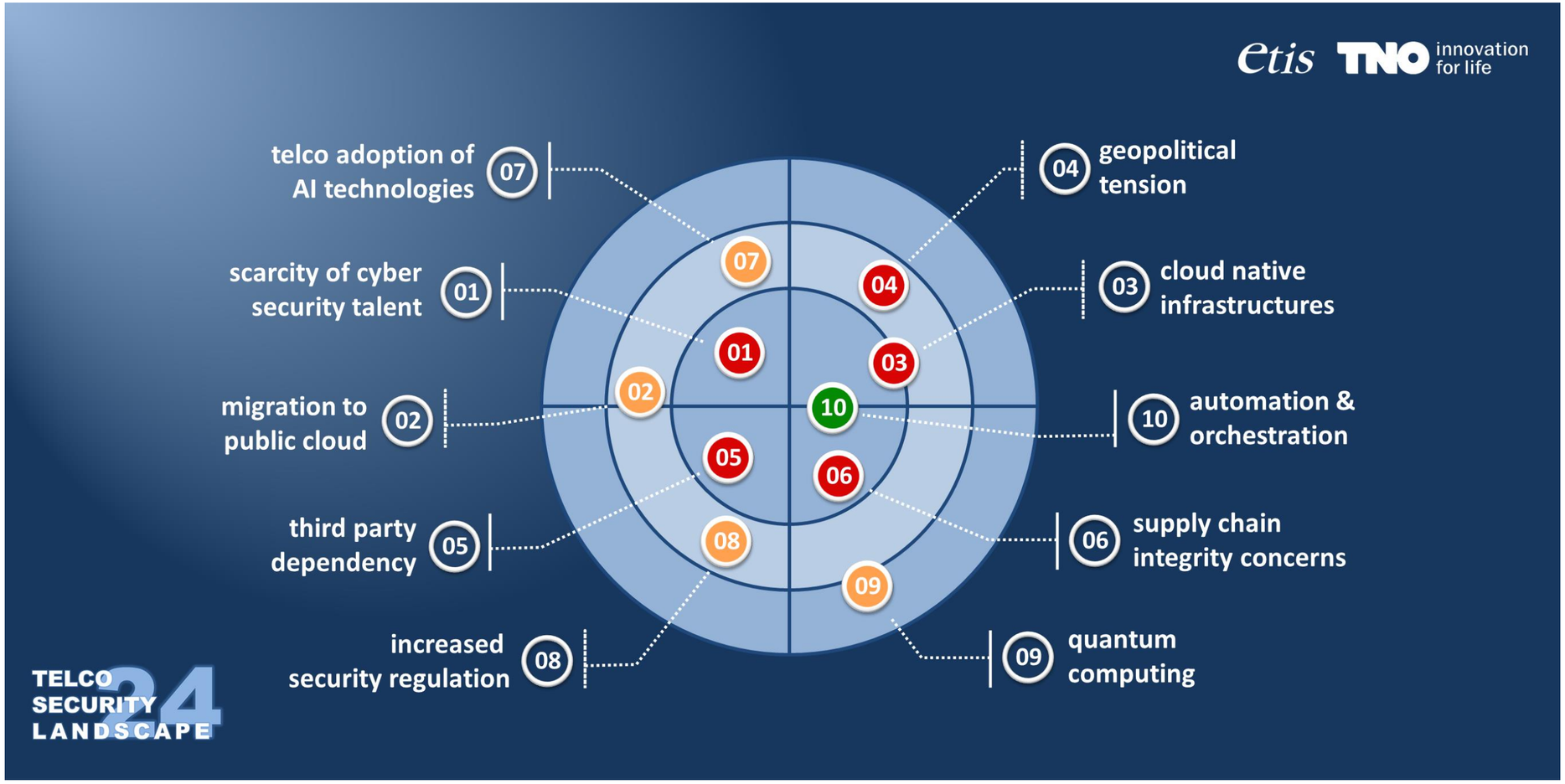
https://www.etis.org/european-telecommunications-isac
isac@etis.org

etis TNO

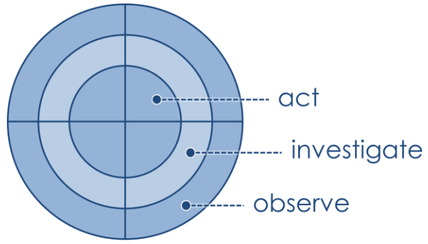
European Telecommunications ISAC

Telco Security Landscape 2024

Updated landscape for 2024



= threat
= opportunity
= both



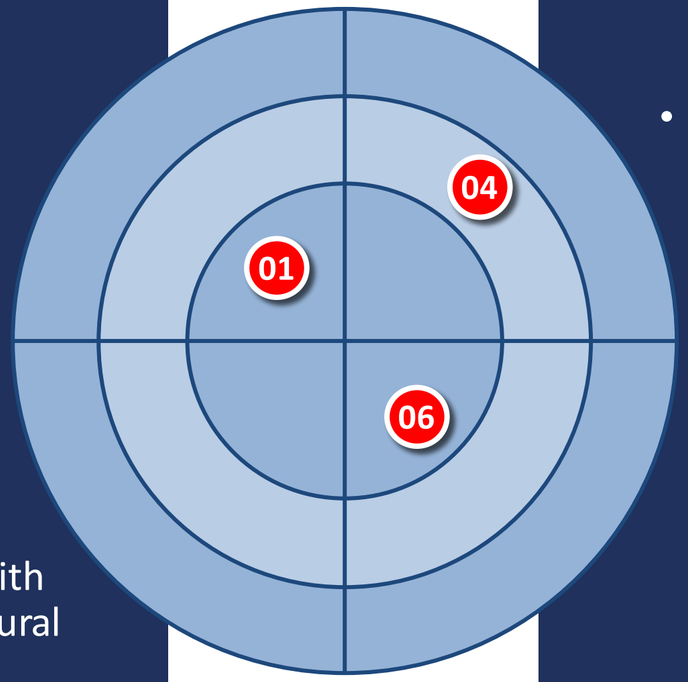
Kept in place from 2024

01 scarcity of cybersecurity talent

- Structural shortage of skilled cyber security workforce
- Need to invest in recruitment and optimise conditions to retain staff for a career in cyber security

06 supply chain integrity concerns

- HW/SW supply chains come with systemic risks that need structural attention
- Initiatives like GSMA's NESAS address the issue to some extent, but do not cover all associated risks (nor all relevant equipment)



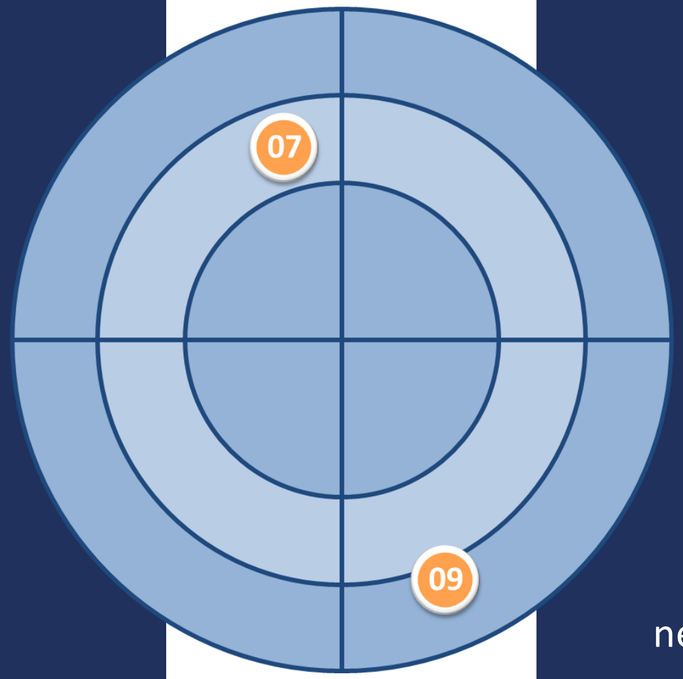
geopolitical tension 04

- Geopolitics can affect availability of specific equipment and (spare) parts or make the energy supply less stable, potentially impacting telco service continuity
- Some governments may impose restrictions on working with specific vendors or providers due to national security concerns

New entries

07 telco adoption of AI technologies

- AI will become prominent in telco network management and 6G. Telcos will need to protect the underlying technology/ algorithms to ensure reliability.
- On a more generic level there is a need to safeguard sensitive data whenever telco employees use publicly available LLMs.
- On the positive side, AI will likely drive fundamental enhancements in cyber defense.



quantum computing 09

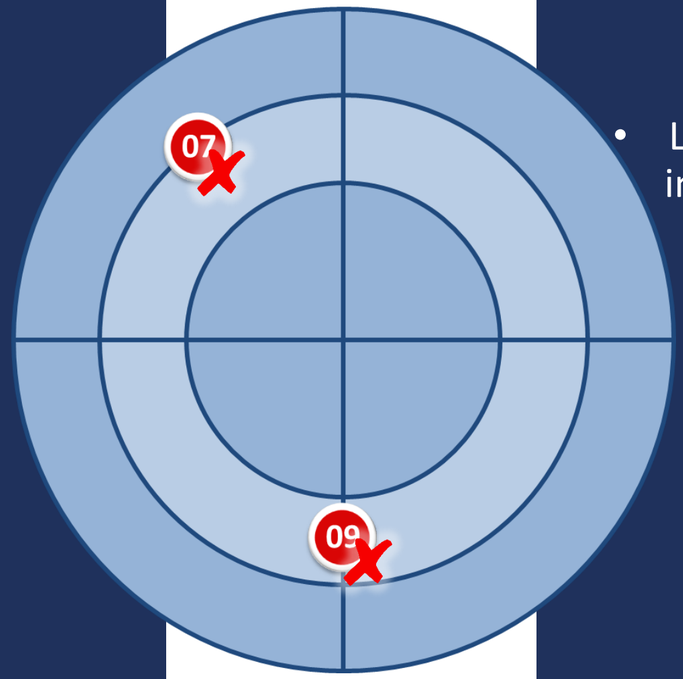
- Much of the crypto that telcos presently rely on is vulnerable to cryptanalysis by quantum computers. Growing sense of urgency to plan for migration to PQC, a.o. in view of “harvest now, decrypt later” threat.
- At the same time quantum computing may offer telcos new opportunities for securing their networks and supplying more secure connectivity services.

Unlucky dropouts

widening of telco eco-system

- Security implications of expanding telco ecosystem, both in technologies (e.g. cloud, OpenRAN) and market players

updated insight:
things have been changing for a few years and it has not become a problem



limitations of legacy equipment

- Legacy alongside newer tech results in complex environment that is hard to protect. Seen as urgent because migration to cloud increases exposure.

updated insight:
problem is diminishing and will likely resolve itself over time

Ascenders and descenders

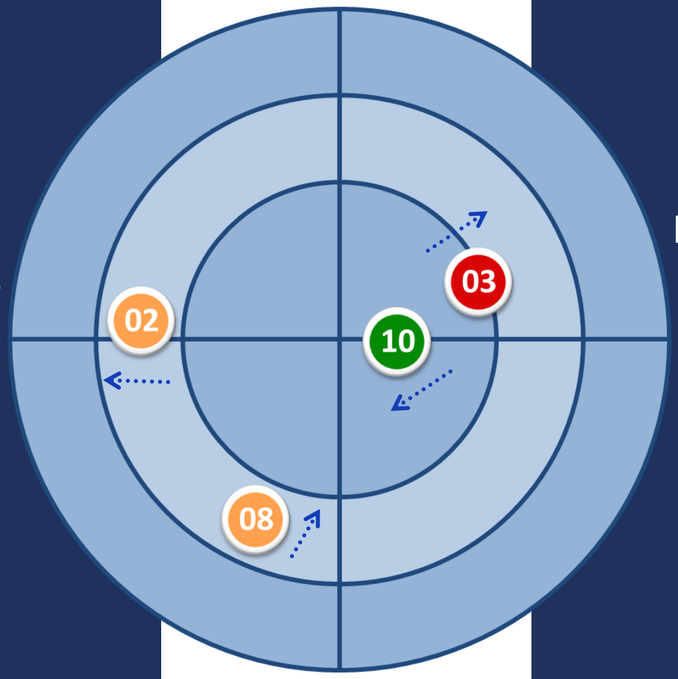
increased priority/ attention

08 increased security regulation

E.g CRA, CER, NIS2, DORA.
More pressure on CIISO teams.
May incentivise elevated internal security and improve product security reliability.
many developments and a lot of impact

10 automation and orchestration

High on the agenda in the monitoring, response and intelligence space,
high on agendas of CISOs and SOC/CSIRT teams



decreased priority/ attention

03 cloud native infrastructure

Requires fundamental rethinking of traditional security models and architectures, and focus on emerging issues (e.g. API sec.).
Many CISO teams likely need to re-skill.
technology and its risks now better understood

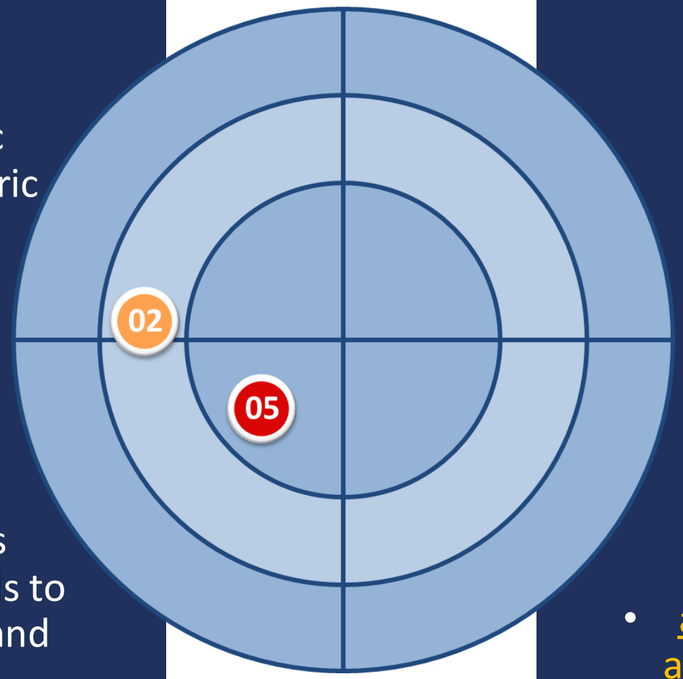
02 migration to public cloud

landscape is clearer;
typically only IT (not TI)

Descriptive refinements

02 migration to public cloud

- Moving telco systems to public cloud implies reliance on generic certifications (e.g. ISO/IEC 27001 or 27017). Need to assess more closely under which circumstances this will suffice.
- Allocation of security relevant responsibilities between telcos and their cloud providers needs to be understood in more detail and appropriately acted upon.
- add: also a source of shadow IT – business known to acquire SaaS outside of regular procurement



third party dependency 05

- Security in core telco ops. often relies heavily on capability of vendors to which particular (maint.) duties are outsourced.
- Governance can be challenging. Will likely become more complex as telcos increasingly integrate native SW dev. pipelines with those of their suppliers
- add: managing (remote) third party access to telco owned infrastructure is challenging, processes put in place to this end are often flawed

Feature article: BT's journey in third party security

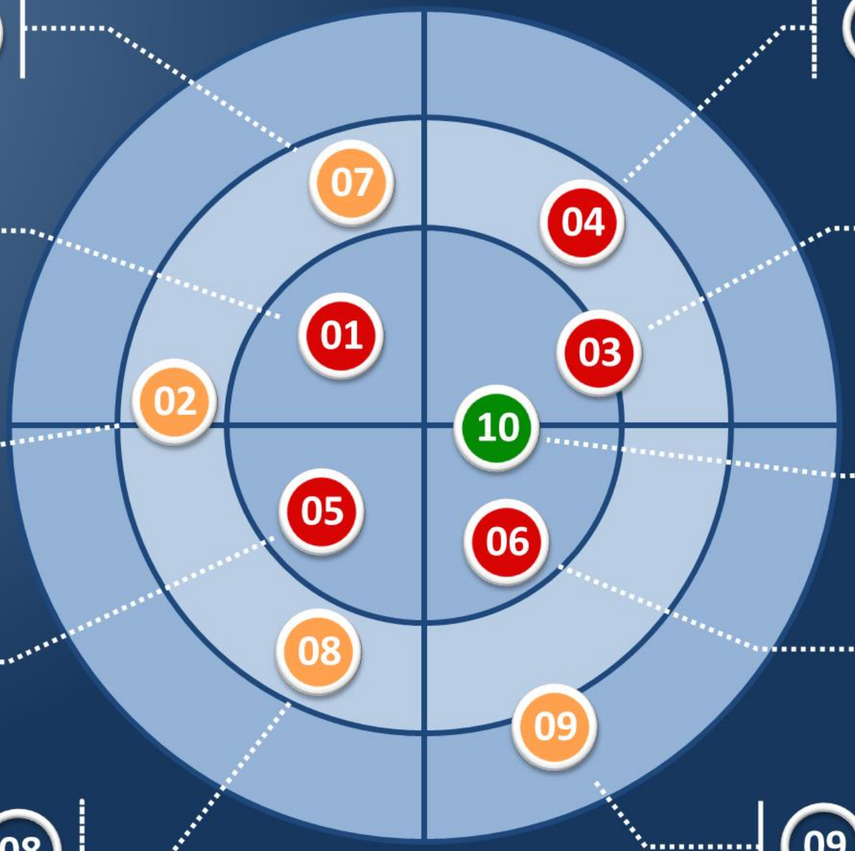
Dominic Wood
Security Governance and Assurance Director at British Telecom

"Third party dependency and Supply chain integrity concerns rightly continue to be near-term risks which all telcos need to act upon.

In fact, the theme of supply chain security features to a greater or lesser extent in all 10 themes within this year's Telco Security Landscape."

- Dominic Wood, BT

etis TNO innovation for life



07 telco adoption of AI technologies

01 scarcity of cyber security talent

02 migration to public cloud

05 third party dependency

08 increased security regulation

04 geopolitical tension

03 cloud native infrastructures

10 automation & orchestration

06 supply chain integrity concerns

09 quantum computing

TELCO SECURITY LANDSCAPE 24

Thank you for your attention

telenor

Rolv R. Hauge
BCM Manager,
Telenor Norway

+47 91138287
rolv.hauge@telenor.no

The Telco Security Landscape 2024 (pub. ed.)
https://www.etis.org/papers

The ET-ISAC
isac@etis.org
https://www.etis.org/european-telecommunications-isac

etis