



Security Conference

Securing the Telecom Business Across IT and Network

Presented by: Dr. Anand R. Prasad

Deloitte.
デロイトトーマツ

18/10/2023



October 18, 2023

Securing the Telecom Business Across IT and Network

Dr. Anand R. Prasad

Deloitte Tohmatsu Cyber LLC

< Confidential >



Contents

- 1 Introduction
- 2 The IT / OT gap in Mobile Network Operators
- 3 The challenge by example of SOC
- 4 Case study
- 5 Conclusions

About Deloitte Tohmatsu Cyber

Deloitte Tohmatsu Cyber LLC

CYBER STRATEGY (Strategy and Transformation)

- Technology transformation
- Growth strategy (Business Transformation)
- Rule formation strategy
- Cyber risk strategy
- Benchmarking against industry standards and best practices
- Secure solution/service design
- Enterprise and network security architecture
- Cyber Risk quantification
- Operation Transformation
- Supply Chain Transformation
- Transformation program
- Organization, HR, and corporate culture transformation

SECURE

- Security assessment
- Infrastructure/Application Protection
- IT Asset Management
- Cloud Environment Protection
- Vulnerability Management
- Identity and Access Authority Management
- Information and Privacy Protection

VIGILANT

- Threat Intelligence
- Cyber Security Monitoring
- Security Analysis
- Red Team Operations
- Purple Teaming

RESILIENT

- Establishment of incident response system
- Incident response (Forensic)
- Crisis management
- Business Continuity Management
- Incident exercises (War Gaming)



Other Business

- Audit & Assurance
- Risk Advisory
- Consulting
- Financial Advisory
- Tax & Legal

About Anand Prasad

Partner, Emerging Technologies & Connectivity Security



Professional roles

- Partner Emerging Technologies
Deloitte Tohmatsu Cyber
- Board of Directors,
A national 5G network in Malaysia
- Senior Security Advisor,
Large Japanese MNO
- CEO and Founder,
A small start up
- Chief Information Security Officer,
Japanese MNO
- Chairman Security Working Group,
3GPP
- Chief Advanced Technologist,
Equipment manufacturer and SI.

Summary of recent achievements

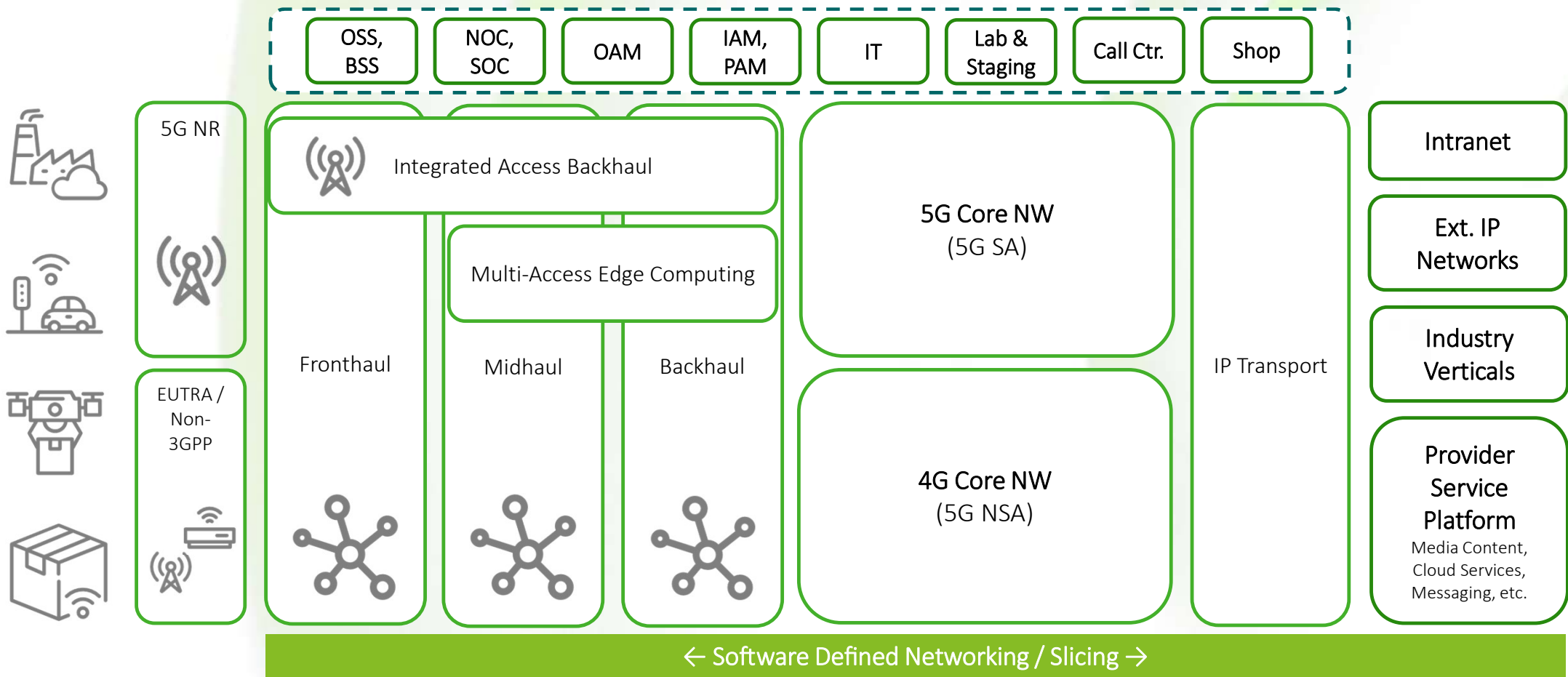
- Leading the Emerging Technologies practice in Deloitte Tohmatsu Cyber LLC.
- Supporting all aspects of a Malaysian 5G wholesale network provider
- Enabled a Japanese operator's first cloud native mobile network launch by delivering all aspects of enterprise, cloud, and mobile network security in under 1 year
- Advised a large Japanese operator on their cyber security transition covering all aspects like IT, ISP, SOC, CSIRT, applications and services
- Delivered the global 5G Security specification through leadership that put business above technology
- Early propagator of 'security as business driver' where security is a driver for business transitions and new business development
- Firm believer in the concept of holistic security, where security is not address piece-wise but as a whole and as part of the entire ecosystem
- Authored 6 books and holds over 50 patents

The IT / OT gap in Mobile Network Operators

Mobile Network Operators have traditionally divided their operations in OT for the network (or operational) technology and IT for their IT services, office IT, and non-network related IT. The impacts to security are still felt today.

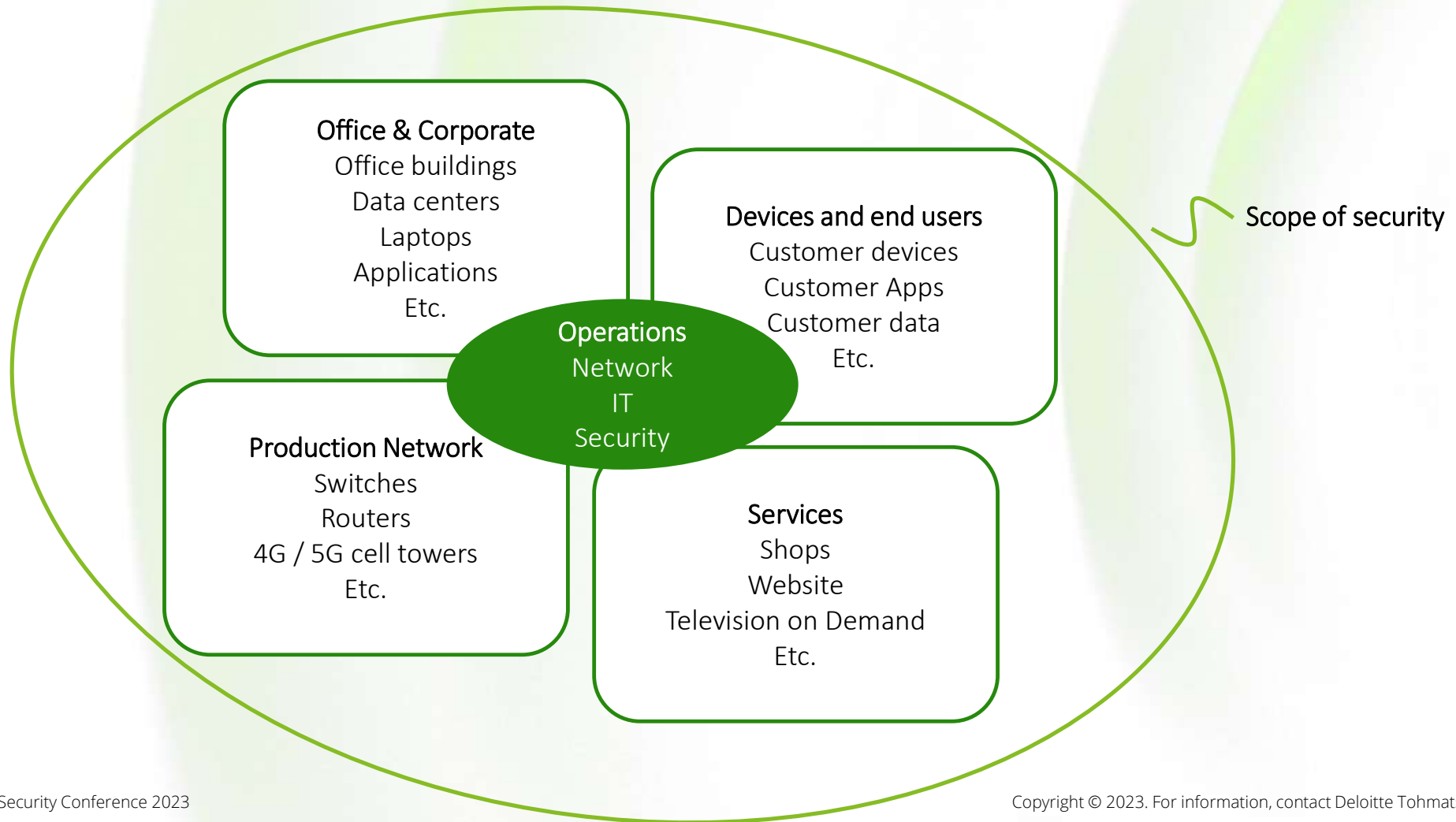
Birds-eye View on Securing Mobile Network

The view that network specialists have



Birds-eye View on Securing a Mobile Network Operator

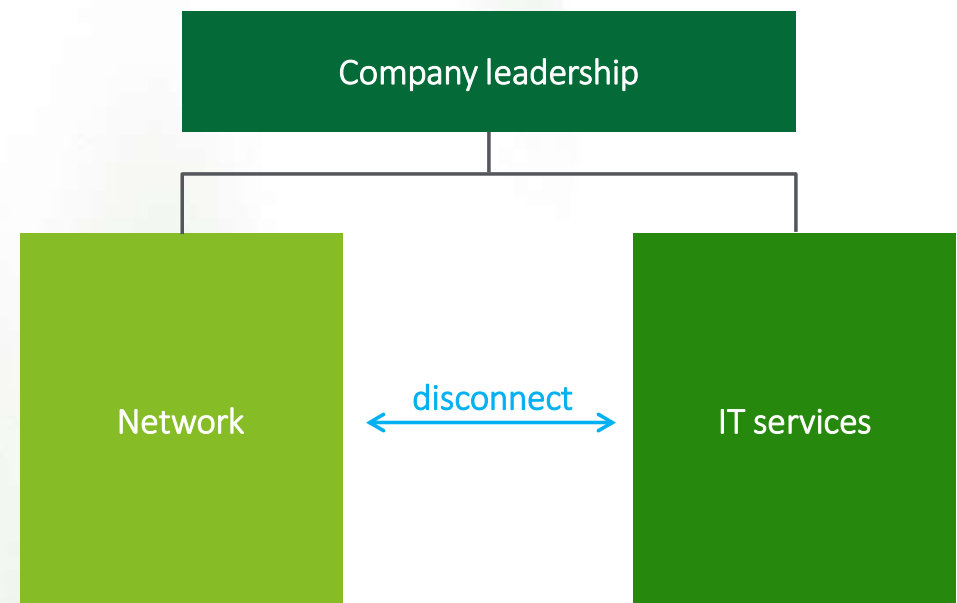
The view that the IT organization has



The network business is traditionally separate from the IT business

Many mobile network operators have traditionally divided their businesses into divisions or business units taking care of the network and other businesses and divisions taking care of other parts.

- From an historical perspective, network deployments are often outsourced, require specialized knowledge and were deployed using hardware.
- This legacy is reflected in how most mobile network operators still operate today. The CTO manages the network, the CIO manages the IT.
- Security teams are either spread over the various businesses or are positioned in the IT divisions, leading to lack of oversight for the network
- However, this way of working does not hold up when deploying a 5G mobile network, which incorporates more and more IT rather than being traditional hardware-based network equipment.



Additionally, there is a false sense of security through standards compliance

To make things worse, compliance with interoperability standards like 3GPP / ETSI is often equated to being secure, leaving the proprietary, closed interfaces under specified and open to attack.

3GPP standards focus on secure interoperability:

- Procedures between UE and the network:
 - Primary authentication
 - Session management
 - Mobility
- Agreement, distribution, and storage of cryptographic keys between mobile device and the network,
- Interfaces and protocols between essential mobile network components,
- Interconnection between different mobile networks
- Interworking between different mobile generations (e.g., 3G, 4G/LTE)

Security of network services & network security capabilities, evolving slowly from generation to generation

NIST, ISO, CIS, etc. focus on securing tech and ops:

- Technology infrastructure, including:
 - Cloud infrastructure
 - Transport networks
 - Network security appliances (firewalls, etc.)
- Management processes and tools
- Operational security, such as:
 - Security hardening
 - Patch management
 - Incident detection and response
- Over-the-top services provided by MNOs or 3rd parties

Security of the entire network technology stack and user data, evolving constantly based on use cases and associated threat

¹ For clarity of the argument, the NESAS and SCAS work was intentionally left out.

Across the industry, security teams report challenges

Security teams report challenges in both the IT security integration as well as managing the network specific security.



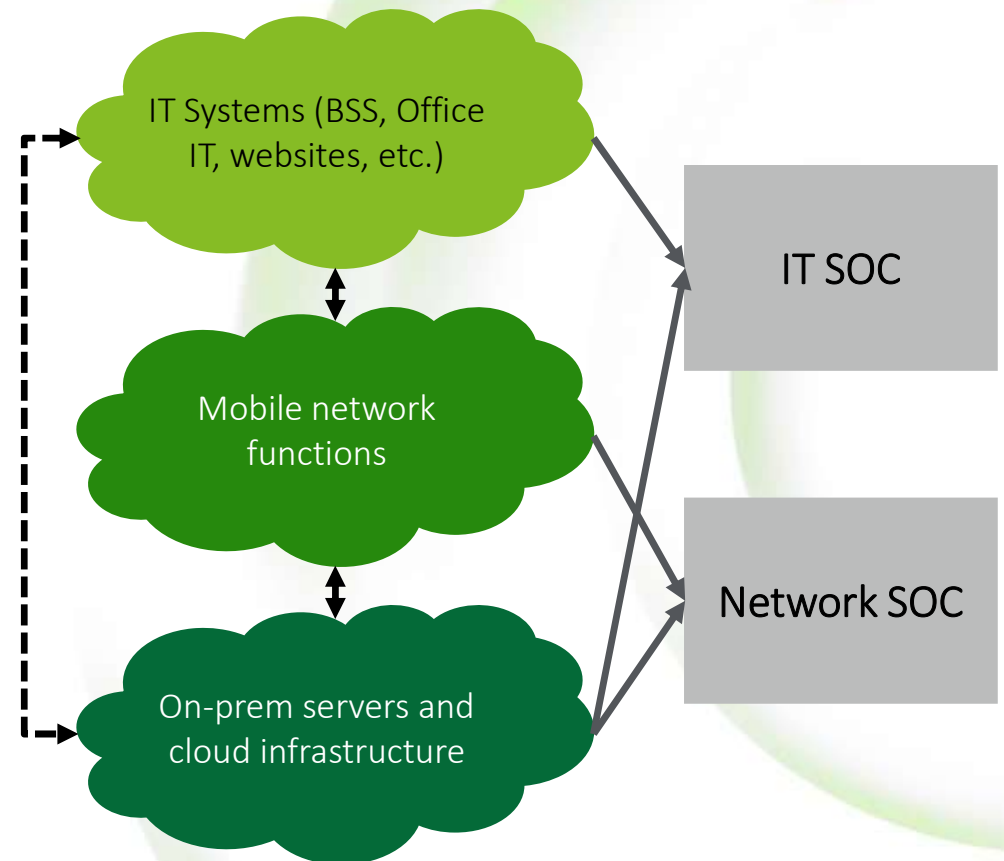
An example

For some Mobile Network Operators, the SOC is divided between Network and IT. We identify issues with that setup.

Example: SOCs are often managed separately and lack established standards

Dedicated SOCs for Network and IT introduce inefficiencies

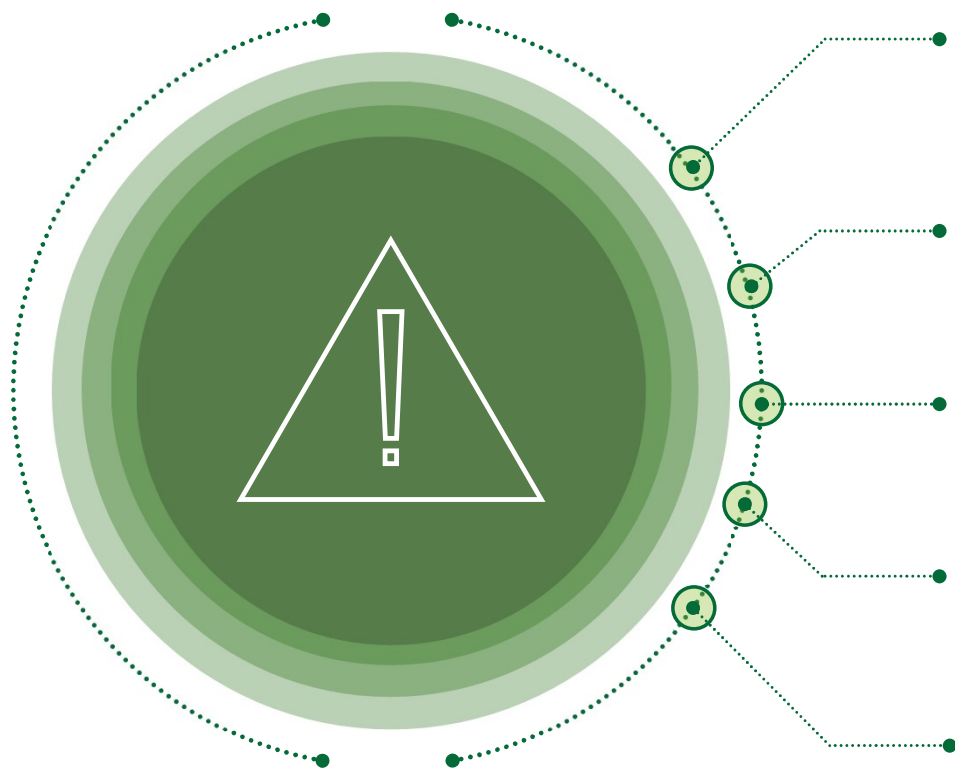
- Although IT, network, and compute infrastructure are all interconnected, security operations are often stuck in silos
- IT SOC and Network SOC are commonly separated in different teams, or worse, the mobile network elements are not enrolled in a SOC at all
- SOC personnel in either of the SOCs has domain-specific focus, and organizational separation hinders close collaboration
- Focus is often on technology, but processes and governance are equally important for efficient detection and response
- Lack of established standards and industry guidelines makes it difficult to assess SOCs against a commonly agreed baseline and impedes further advancements¹



¹ Security Operations Center: A Systematic Study and Open Challenges (DOI: [10.1109/ACCESS.2020.3045514](https://doi.org/10.1109/ACCESS.2020.3045514))

Separate security operations can pose significant challenges

Separation can lead to lack of visibility, increased effort, and impede incident response



Lack of visibility

Malicious actors don't move along defined domain perimeters. Unless a SOC has visibility into data from all systems, it is bound to be blind on one eye.



Lack of context

Not being able to correlate events from different domains can make it harder to pick up on anomalies, further increasing the detection time.



Increased effort

Operating multiple SOCs in parallel means parallel work, added potential for process inconsistencies, and human error.



Delayed incident detection

Impaired vision and organizational hurdles can delay detection time in the event of a security incident.



Inconsistent response

Without alignment across different SOCs, executing a consolidated incident response is going to be a challenge.

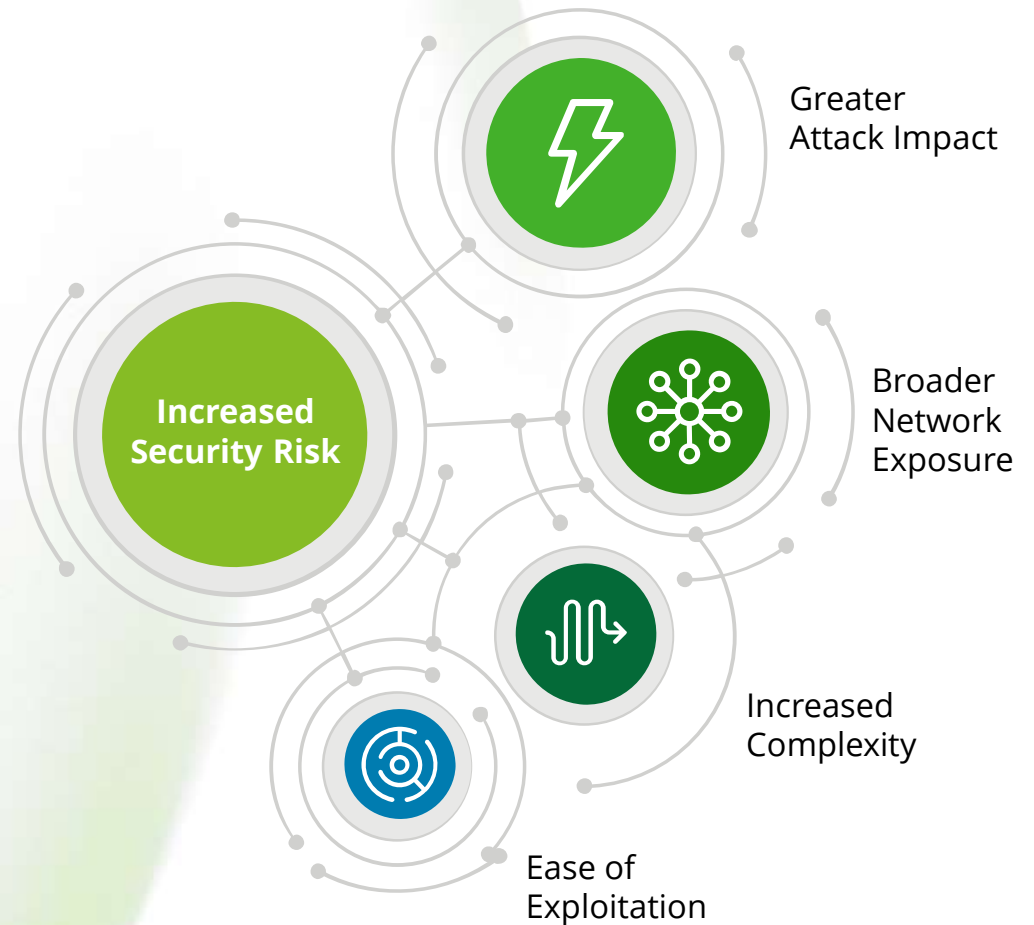
Relevance to 5G mobile networks

5G mobile networks leverage a plethora of web technologies, are designed to live in the cloud, and have a much larger exposure to the outside world. As such, adopting IT security technologies for 5G mobile networks is imperative to successful and cost-effective security.

5G is about a paradigm shift that exposes telecom operators to new risks

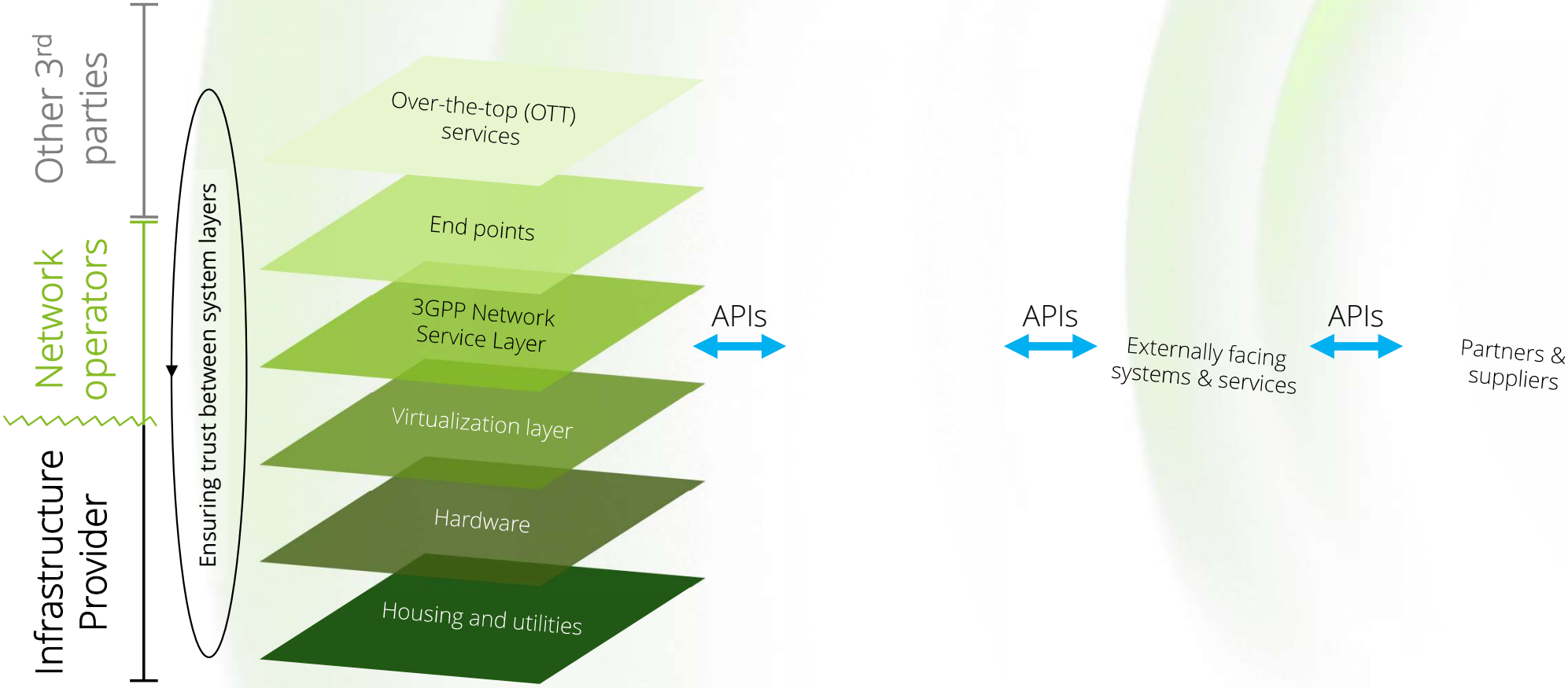
Increased risks due to greater attack impact, broader exposure, increased complexity

- More so than a technological revolution, 5G is about a paradigm shift in the mobile industry's mindset
- Flexible services, seamless integration with different parties, effective & easy to use security – everything successful internet platforms offer is expected from modern mobile networks
- Change in expectations has substantial impact on MNO business models and how to secure them:
 - Diversified applications and service offering
 - Data and service exposure via public APIs
 - Low entry barrier for new, inexperienced tech suppliers
- Managing increased complexity of interconnected, constantly changing network and IT deployments is the make-or-break issue for MNO security teams



The 5G threat landscape also evolved and includes more IT-like security threats

While it would be easy to look at 5G as just another generation, its level of integration, its technology diversity, and the resulting rise in complexity introduce additional challenges in terms of to attack surface management.



Network equipment itself is also increasingly built on generic IT

With the increase of web technologies, the increase of less experienced vendors, and the increase in virtual appliance, also the use of off the shelf IT has increased. And so must security.

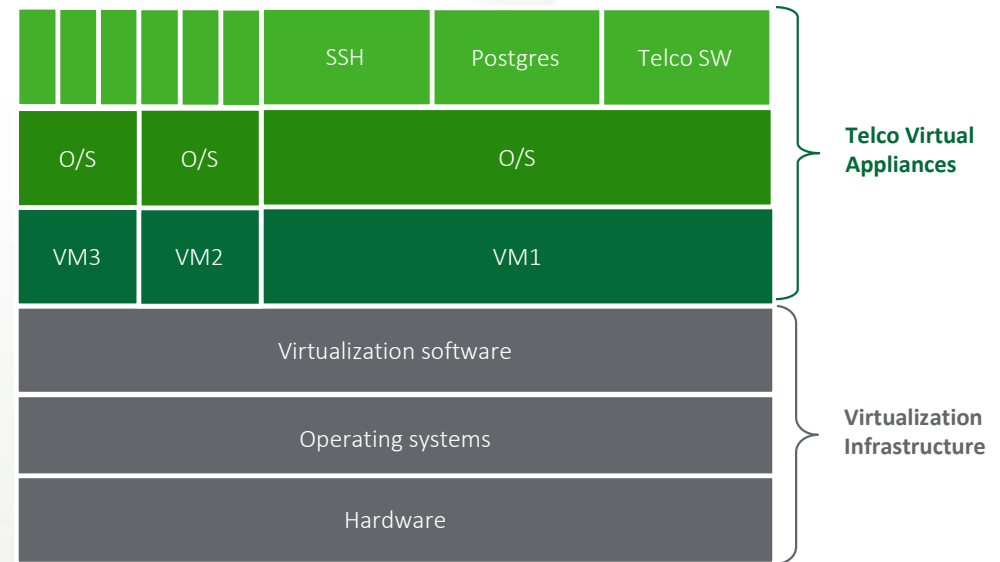
The increase of generic components, requires security teams to rethink the way they approach security of their network. The traditional reliance on interoperability standards covers only a small portion and a more generic approach will be required.

A convergence is required for generic parts:

- Generic security requirements like identity and access management, cryptography, certificates, trusted CAs, etc.
- Security baseline requirements for operating systems, web servers, databases, remote shells, etc.
- Integration into generic security tooling, such as log collection, sending alerts, monitoring, etc.

Specific parts need to be carved out for:

- The telco specific software security
- Configurations of security settings from the standards



Towards unified controls framework & converged operations

Unifying the security controls is the way forward, but how to do that is a problem. Existing frameworks are either too generic, too simple or too complex. Finding the middle road is the key here.

The available frameworks are not sufficient

In IT security, the NIST CSF is the golden standard, but for 5G networks no suitable framework exists, despite very good attempts by both GSMA and ENISA for example.

NIST CSF

The NIST CSF is arguably the most successful security framework available to CISOs.

The advantages are:

- Widely adopted in the industry
- Easy to find expertise
- Sufficiently generic to be applicable to many different IT environments

The shortcomings for 5G networks:

- Too generic for specific telco security needs
- Generic assessments, maturity scores, etc. do not reveal real problems on each individual layer.

GSMA best practices

GSMA publishes documents like FS.31 that are focused on the industry and are specific for mobile networks

The advantages are:

- Written by industry experts
- Applicable for network security
- Focus on controls relevant for mobile network operators

The shortcomings:

- Often the controls are too simple
- Not mapped to existing control sets like NIST or ISO
- Users need to take their specific environment into account

ENISA

The ENISA 5G Controls Matrix is arguably the most comprehensive list of security controls for 5G networks.

The advantages are:

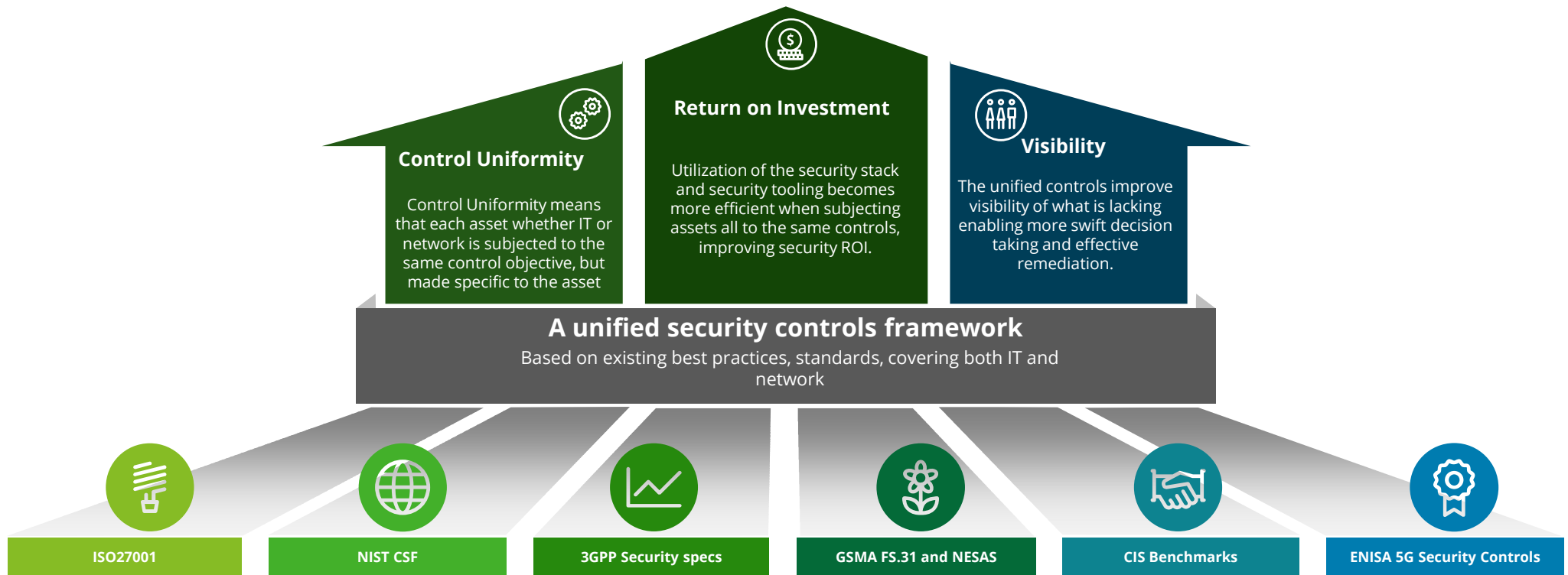
- Sourced from industry standards
- Contains over 400 controls
- Already mapped to other standards like ISO and NIST

The shortcomings:

- Mixes well defined controls with controls from industry specs with less than desired quality
- Overwhelming number of controls that need to be filtered.

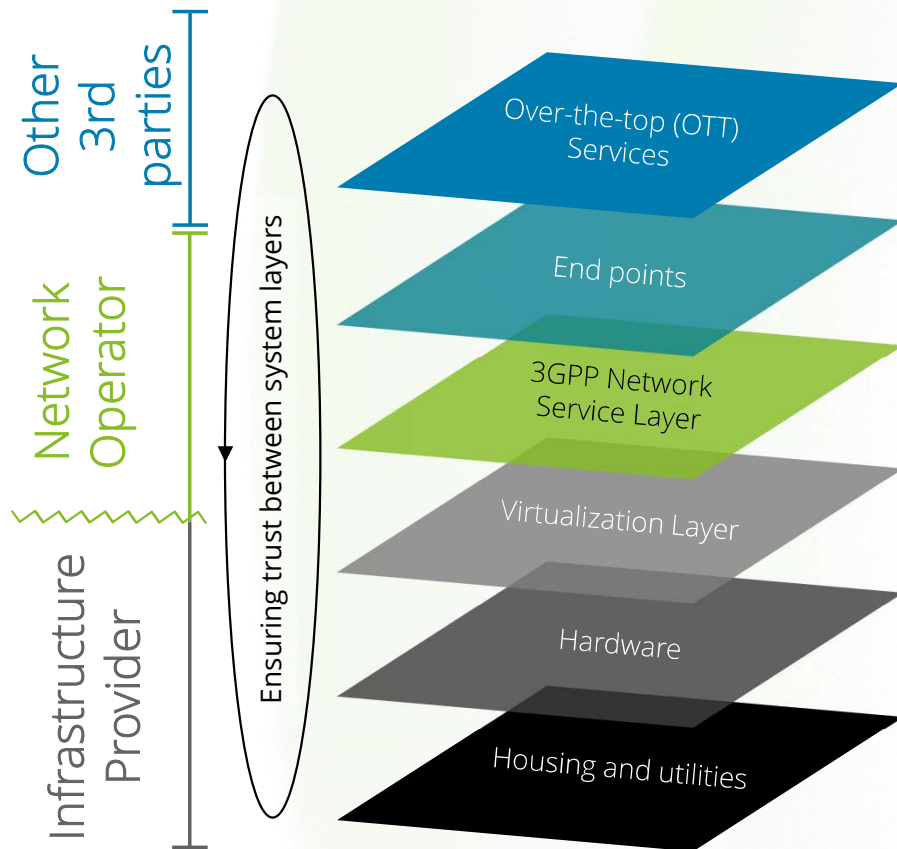
Building on the existing frameworks while taking the special situation into account







We constructed a single controls framework based on the existing one. While aligning with NIST and ISO, we included and deduplicated the controls from the other sources, such as 3GPP, GSMA, CIS, and ENISA.



Framework coverage includes the various layers

The 5G Security Capabilities Framework distinguishes the layers in a typical deployment to allow to see which control applies where and in what way



	OTT Applications	Applications and services provisioned on external infrastructure. Mobile network provides mere connectivity.
	Third-Party Software	Applications and services integrated to some extent with the mobile network (e.g., via network exposure or MEC). May be operated by the telecom service provider or third-parties.
	3GPP Security	Security functionality, protocols, and procedures described in the 3GPP technical specifications. Providing the tools for basic access control and protection of information transported.
	Virtualization Security	Validating the provenance of workloads. Enforcement of resource limitations. Ensuring isolation of workloads between each other and towards the host system.
	Hardware Security	Hardware-supported security functionality, serving as a root of trust, enabling secure credential storage of, and execution of sensitive computations.
	Physical Security	Protecting physical network infrastructure from sabotage and physical damage. Safeguards against natural disasters to ensure availability and business continuity.

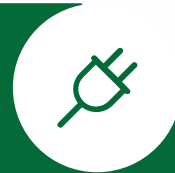
Benefits are expected when using a single control set across IT and Network

Uniform security posture, increased management visibility, and converged security operations are some benefits that are to be expected from using a uniform control framework



Uniform posture

- Each assets is subject to the same controls, eliminating potential weak links
- Vulnerabilities can be addressed across the stack, mitigating where most efficient and effective.



Increased visibility

- Management visibility improves when reporting is unified across network and IT
- Operational visibility improves when all assets are subject to the same monitoring and logging requirements



Converged Operations

- Converging operations between various operational security teams is more efficient for the organization.
- A single 'pane of glass' view can be obtained, allowing faster detection and incident response.

Deloitte.

デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Group LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With approximately 17,000 people in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp/en.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of DTTL, its global network of member firms, or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2023. For information, contact Deloitte Tohmatsu Group.

Copyright © 2023. For information, contact Deloitte Tohmatsu Cyber LLC.



IS 669126 / ISO 27001



BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited