



情報セキュリティ監査- サイバーリスクの観点から

Information security assurance

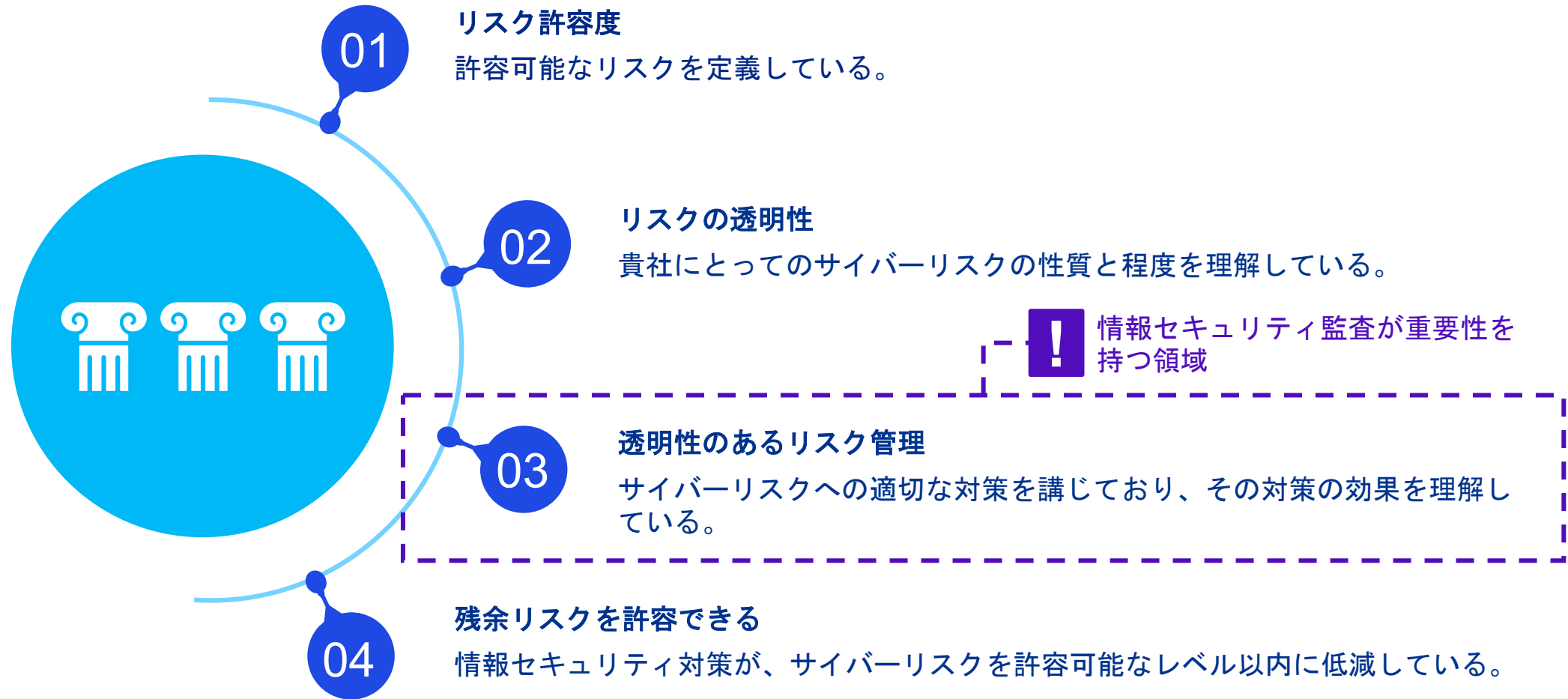
From a cyber risk perspective

Laszlo Hargitai

Senior Manager, KPMG cyber security consulting

May 15, 2024

「良い」サイバーセキュリティの柱



The pillars of a „good“ cybersecurity



情報セキュリティ視点による事業およびIT戦略

主な検討課題:

- どの事業プロセスにITの利活用が必要か？
- どのレベルのITサービスが必要か？
- IT需要のどの部分を外注し、どの部分を内製すべきか？
- どのアプリケーションあるいはシステムを内部で開発すべきか？外部に委託すべきか？
- 事業が個別に開発されたソフトウェアやハードウェアにどの程度依存しているか？

これらの課題に対する答えが用意できた時 ...

... どの程度の透明性を諦めることができるか？

- サイバーリスク
- セキュリティ管理

On-Prem	IaaS	PaaS	ASP	SaaS
Application	Application	Application	Application	Application
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	ACME社	Servers
Storage	Storage	Storage	クラウドソフトウェアの開発者／プロバイダー	Storage
Network	Network	Network	Network	Network
Physical Env.	Physical Env.	Physical Env.	Physical Env.	Physical Env.

内部運用／開発

外部運用／開発

Your business and IT strategies from the internal infosec view

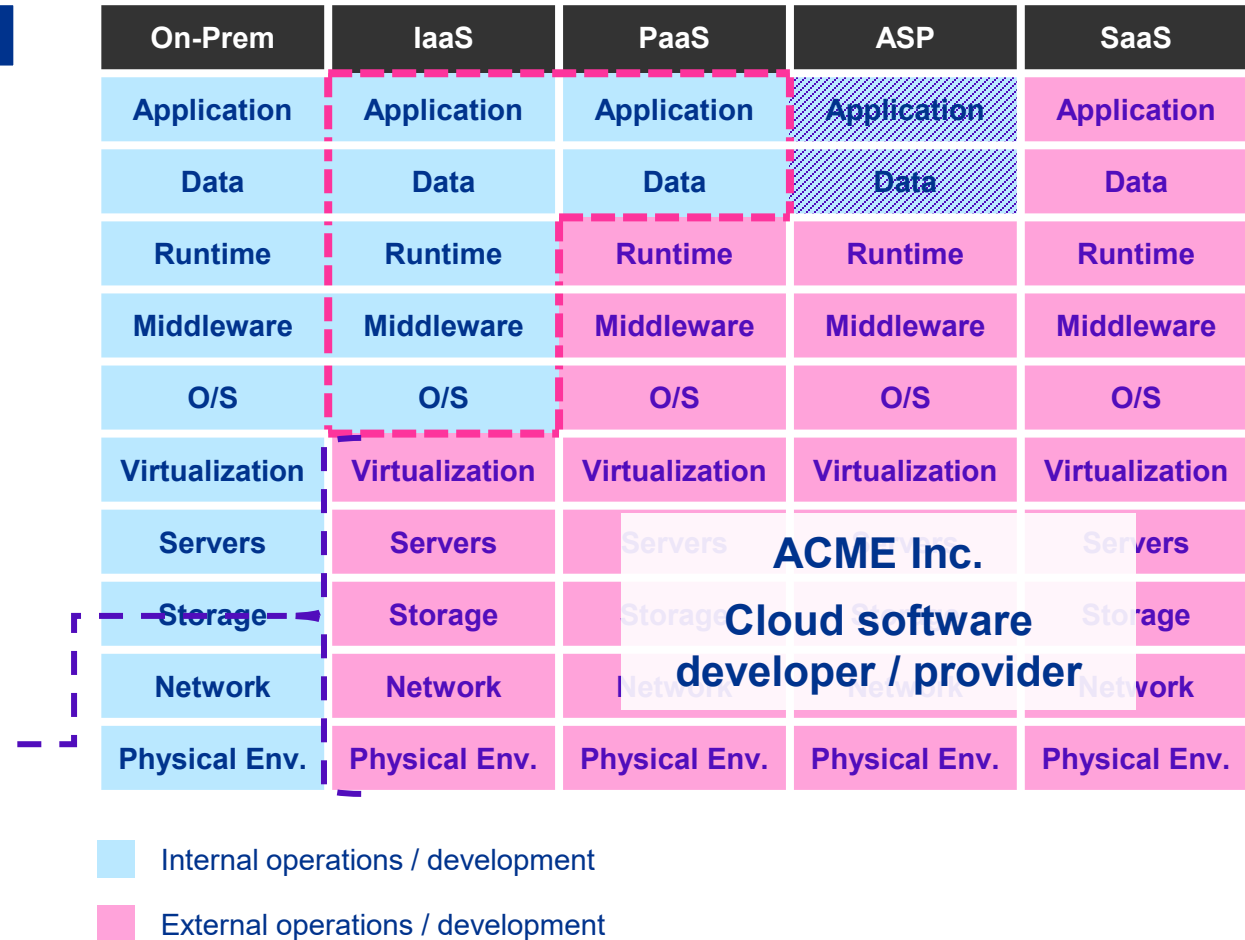
Core questions:

- Which business processes need IT support?
- What level of IT services are necessary?
- Which parts of IT need to be outsourced and retained?
- Which applications / systems are developed internally and externally?
- To what extent depends your business on individually developed software / hardware?

If these decisions have been made ...

... **how much transparency did you give up (even if not deliberately):**

- **regarding cyber risks?**
- **regarding security controls?**



Your business and IT strategies from the external infosec view

主な検討課題:

- どの事業プロセスにITの利活用が必要か？
- どのレベルのITサービスが必要か？
- IT需要のどの部分を外注し、どの部分を内製すべきか？
- どのアプリケーションあるいはシステムを内部で開発すべきか？外部に委託すべきか？
- 事業が個別に開発されたソフトウェアやハードウェアにどの程度依存しているか？

これらの課題に対する答えが用意できた時 ...

... どの程度の透明性を諦めることができるか？

- サイバーリスク
- セキュリティ管理

On-Prem	IaaS	PaaS	ASP	SaaS
Application	Application	Application	Application	Application
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Network	Network	Network	Network	Network
Physical Env.	Physical Env.	Physical Env.	Physical Env.	Physical Env.

ACME社の顧客

内部運用／開発

外部運用／開発

Your business and IT strategies from the external infosec view

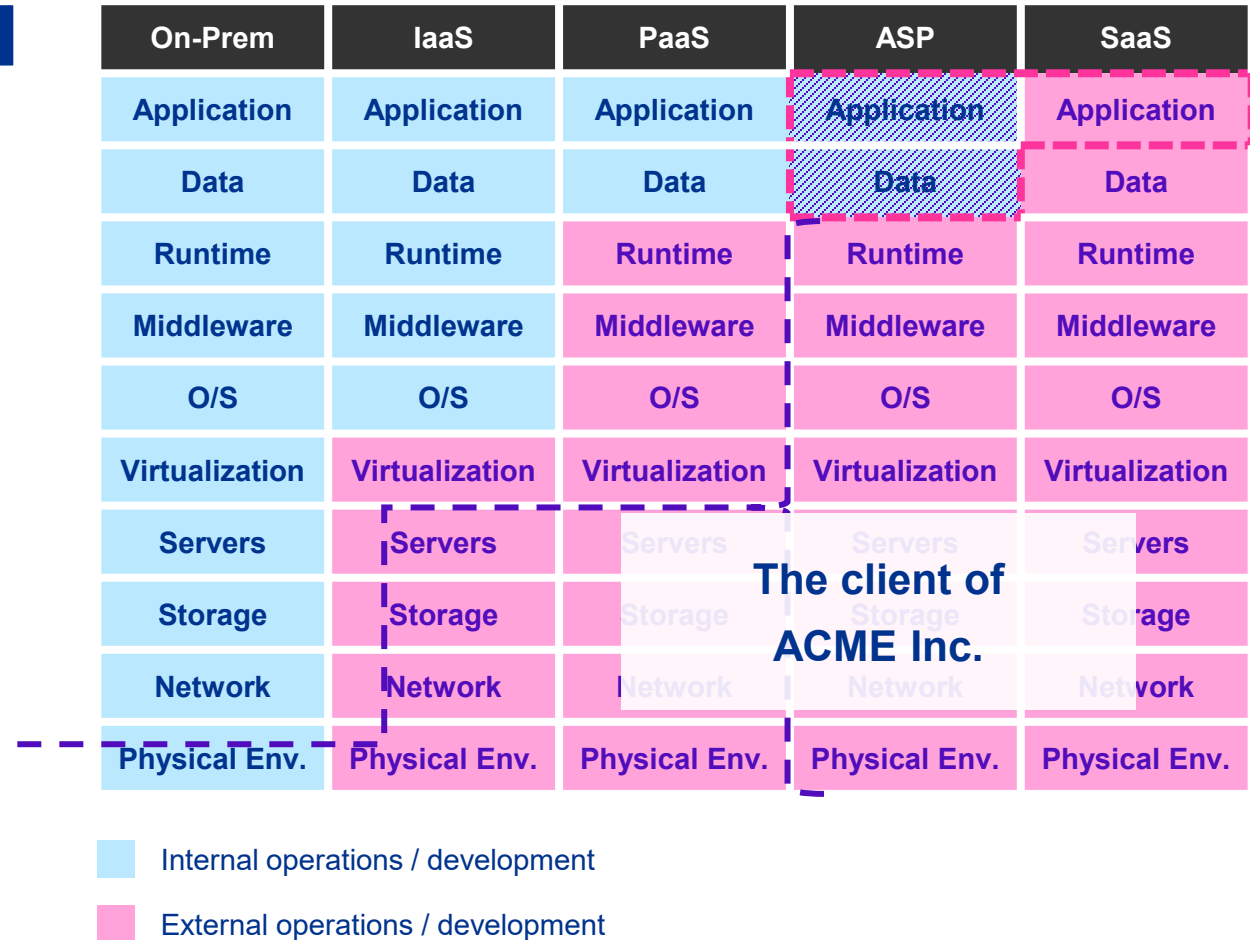
Core questions:

- Which business processes need IT support?
- What level of IT services are necessary?
- Which parts of IT need to be outsourced and retained?
- Which applications / systems are developed internally and externally?
- To what extent depends your business on individually developed software / hardware?

If these decisions have been made ...

... **how much transparency did you give up (even if not deliberately):**

- **regarding cyber risks?**
- **regarding security controls?**



サプライチェーンと情報セキュリティ監査

ACME社の顧客

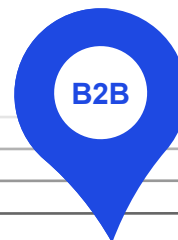
ACME社
クラウドソフトウェア開発／提供

ACME社のベンダー、サブコ
ントラクター



ACME社の顧客は最終顧客か
らの信頼獲得を意図して、
ISO-27001 を取得

- ISO-27001



クラウドソフトウェアのプロ
バイダーは、複数の認定ある
いは監査報告書を取得:

- ISO-27001
- ISAE-3000 監査報告書



クラウドインフラのプロバイ
ダーは、数種類の情報セキュ
リティ認定あるいは監査レ
ポートを取得:

- ISO-27001 / ISO-22301
- ISAE-3000 Assurance Report
- PCI-DSS

貴社事業
が監査対
象事業に
該当する
場合

NIS-2 監査報告書

NIS-2 監査報告書

NIS-2 監査報告書

Supply chain and infosec assurance view

Client of
ACME Inc.



The client of ACME Inc. is ISO-27001 certified, this certification is in use to establish trust of the ultimate customers:

- ISO-27001

ACME Inc.
Cloud software developer / provider



The cloud software provider applied multiple certifications / assurance reports:

- ISO-27001
- ISAE-3000 Assurance Report

Vendor / subcontractor of
ACME Inc.



The underlying cloud infrastructure provider has several infosec certifications and assurance reports:

- ISO-27001 / ISO-22301
- ISAE-3000 Assurance Report
- PCI-DSS

If your
business
is in a
covered
sector



NIS-2 audit report

NIS-2 audit report

NIS-2 audit report

NIS-2指令の概要:適用対象

欧州の新しい「ネットワークおよび情報セキュリティ指令（NIS-2）」はEUの重要なインフラのレジリエンスを確保すべくより包括的なアプローチをとっている。

重点分野



ガバナンス

指令20条は、対象となる企業やその意思決定機関にガバナンス上の要件を設定



リスクマネジメント

指令21条は、サイバーセキュリティリスク管理策に関する要件を規定



報告

指令23条は、サイバーセキュリティに関する事件／事故が発生した場合の報告義務を定めている。

罰金

最重要な企業 → €10m or 世界売上の2%

重要な企業 → €7m or 世界売上の1.4%

どちらか大きい金額



© 2024 KPMG Advisory Ltd., a Hungarian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

対象となる業種

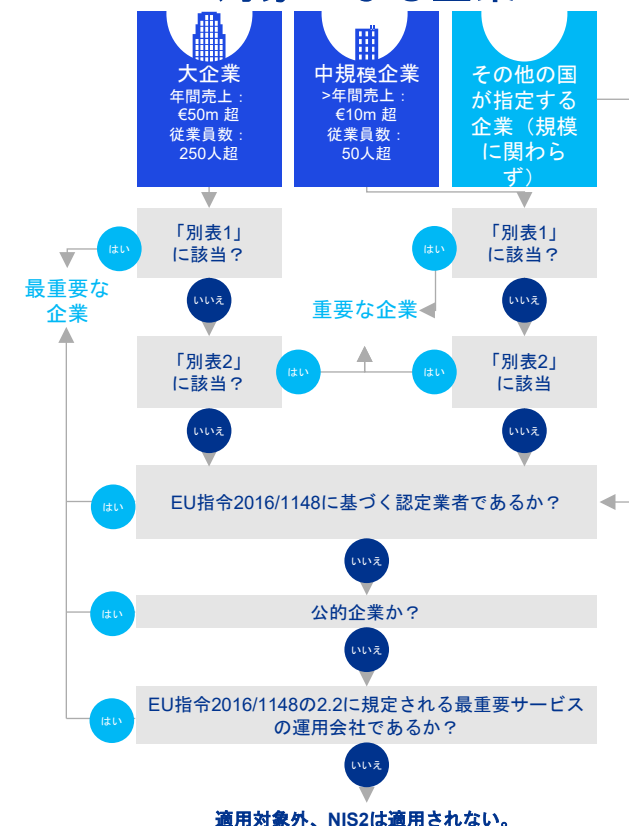
「別表1」に規定される業種



「別表2」に規定される業種



対象となる企業



導入スケジュール

- 2022年12月 | NIS2 署名
- 2024年10月 | 詳細な要請事項の決定および施行
- 2025年1月以降 | 監査人によるレビュー

NIS-2 overview: scope

The EU's new Network and Information Security Directive (NIS2) is taking a more comprehensive approach to ensure the resilience of EU critical infrastructure.

Focus areas for entities



Governance

Art. 20 sets out governance requirements for entities and their management bodies



Risk management

Art. 21 determines requirements for cybersecurity risk-management measures



Reporting

Art. 23 imposes reporting obligations on entities for incidents

Penalties for non-compliance

Essential entities	→	€10m	or	2% of total worldwide annual turnover
Important entities	→	€7m	or	1.4% of total worldwide annual turnover
<i>whichever is higher</i>				

Sectors in scope

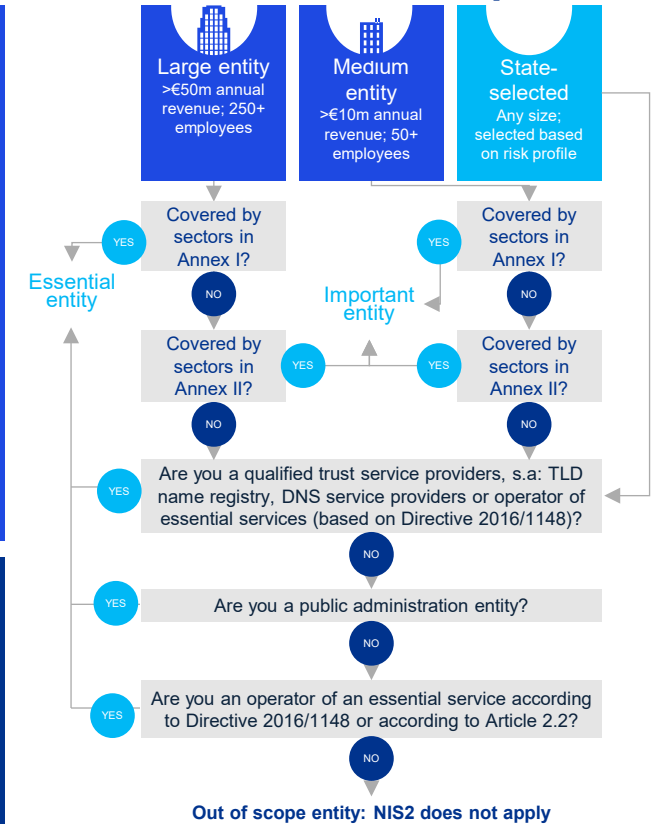
"Annex I" entities



"Annex II" entities



Entities in scope



Implementation timeline

- Dec 2022 | NIS2 signed
- Oct 2024 | Detailed requirements & in effect
- From Jan 2025 | Auditor reviews

NIS-2 指令の概要: 管理項目(ハンガリー)

ハンガリー政府当局は、NIST 800-53 r5の枠組みに基づいて、NIS-2指令の国内への導入に際しての管理項目を発表した。これは、NIS-2指令の導入およびその後のリスク管理手法およびセキュリティ管理の監査人によるレビューの基礎となるものである。

NIST 800-53 の セキュリティ 管理領域

リスクマネジメント

- リスクアセスメント
- 評価、権限付与、モニタリング
- 計画策定
- プログラム管理
- 個人を特定可能な情報の処理と透明性
- サプライチェーンリスク管理

技術的なセキュリティ

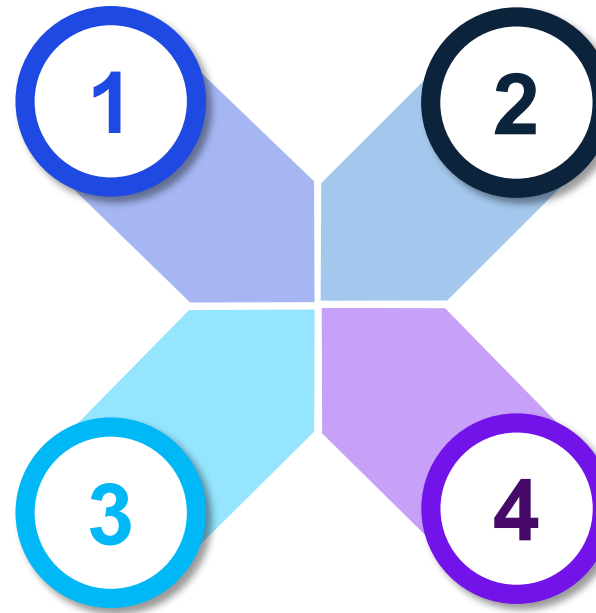
- アクセス管理
- 監査および信頼性
- 特定と立証
- メディア対策
- 物理的・環境的な防御
- システムおよび通信上の防御
- システムおよび情報の完全性

IT・セキュリティの運用

- 設定管理
- 危機対策
- 事件・事故への対応
- メンテナンス
- システムおよびサービスの取得

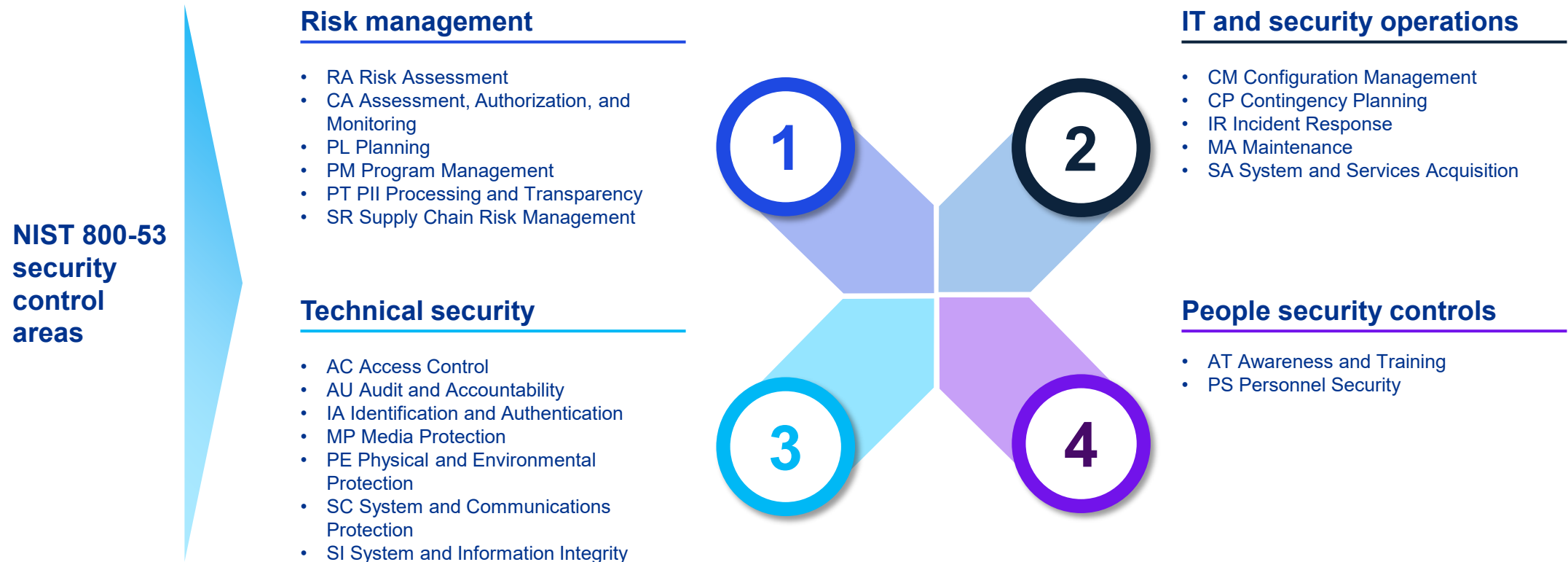
人的セキュリティの管理

- 認知の向上と研修
- 人事上のセキュリティ



NIS-2 overview: controls (HU)

The Hungarian authority published a control catalogue for the national implementation of the NIS-2 directive based on the NIST 800-53 r5 framework. This builds the base for the NIS-2 implementation and, at a later stage, for the audit review of the risk management measures and security controls.



情報セキュリティの認定および監査の枠組み

国際/国内規制

- **EU NIS-2指令**: 最重要および重要業種に属する企業
- **EU DORA**: 金融機関を対象としてデジタルオペレーションの復元力向上を意図
- **EU MDR (医療機器規則)**: ソフトウェアや情報セキュリティに関する規定
- **EU 一般データ保護規則 42条**: (任意の) 認定制度

業界標準

- **PCI-DSS** → 決済カードの取り扱いに関する標準
- **SWIFT 顧客セキュリティプログラム** → SWIFTネットワークに接続する企業のための情報セキュリティ上の標準
- **TISAX** → 自動車業界サプライヤーのための情報セキュリティ上の標準

業界横断的な標準および枠組み

標準:

- **ISO-27000**: 情報セキュリティ管理 **ISO-23000**: 事業の継続性
- **ISO-81000**: ソフトウェアのサイバーセキュリティ

フレームワーク:

- **NIST SP 800-53 / CSF**
- **CIS** 重要なセキュリティ管理
- **ISF**

監査・報告

- **ISAE 3000 / 3402**: 以下に関する独立外部監査人による年次監査報告書:
 - 内部リスク管理
 - 持続可能性
 - 法令遵守
- 情報セキュリティおよびデータ保護を含む

↑ Please note, that this is a non-exhaustive list with examples ↑

Infosec certification and assurance frameworks

International / national legislation

- **EU NIS-2:** businesses in essential and important sectors
- **EU DORA:** organizations providing threat-led penetration tests
- **EU MDR (Medical Device Reg.):** adherence to software / information security requirements
- **GDPR Art 42.** certification mechanisms (optional)

Sector-specific standards

- **PCI-DSS** → secure handling of payment card holder data
- **SWIFT Customer Security Program** → information security requirements for entities connected to the SWIFT network
- **TISAX** → information security requirements for automotive suppliers

Cross-sector standards and frameworks

Standards:

- **ISO-27000:** information security management **ISO-23000:** business continuity
- **ISO-81000:** cyber-security of health software

Framework:

- **NIST SP 800-53 / CSF**
- **CIS Critical Security Controls**
- **ISF Standard of Good Practice 2024**

Assurance reporting

- **ISAE 3000 / 3402:** Yearly assurance report provided by an independent auditor about:
 - Internal risk controls
 - Sustainability
 - Legal compliance→ ... incl. information security and data protection

↑ Please note, that this is a non-exhaustive list with examples ↑

課題-戦略的管理

より複雑になる要請事項

国内およびEUレベルでの様々な規制が情報セキュリティおよびデータ保護に関する要求事項を規定するようになっていく中、どの規制への遵守が必要であり、どの規制の認定を取得するのが得策か？

単に対処療法的に、自社が該当する要請・遵守事項に対応、あるいは認定を取得していくと、多大なコスト増を招くことになります。

増加する経営責任

新規の各種規制（例えばNIS-2）には、企業の経営者の責任（個人に対する罰則）が規定される傾向にあります。経営者の責任には、取引業者等の第三者のリスクを管理する適切な枠組みの構築が含まれます。

- ITサービスプロバイダーからどのような認定あるいは報告書を取得するか？
- サプライチェーン全体をカバーする情報セキュリティ管理をどのように確かなものにするか？（例）起用しているITサービスプロバイダーのセキュリティー遵守報告および当該報告の継続的な管理にどの程度の投資を行うか？
- 起用しているITサービスプロバイダーの認定が取り消された、あるいは、限定的な保証しか得られなかった場合の対応をどうするか？
- 後者のケースにおいて：どのぐらいの期間、増加したリスクレベルを許容するか？

Challenges – strategic management view

Increased complexity of requirements

More and more legislations at the national and EU level define information security and data protection requirements, for which the attestation of compliance is necessary or advisable.

The mere decision (and follow-up) about which legislations, requirements and certifications are relevant for a given organization, lead to increasing costs. This is also conditional on the business strategy (→ e.g. B2G, critical infrastructure provision, B2B, oversees operations) and on the IT strategy (→ digital transformation, cloud).

Elevated management liability

The liability of the senior management gets more attention in the new legislations, accompanied by personal sanctions (e.g. in NIS-2). This liability includes, among others, the establishment of an appropriate third-party risk management framework:

- **What certifications / assurance reports do you require from your IT providers** (if any)?
- **How do you ensure, that your infosec controls cover the whole supply chain**, e.g. how much do you invest in the security compliance reporting of your IT providers and in the regular control of these reports?
- **How do you react, if the infosec certification of an IT provider gets revoked**, or a limited assurance report is issued?
- In the latter case: how long do you remain at the same IT provider, accepting the elevated risks?

課題-戦略的管理

サプライチェーンの複雑化

貴社が、販売・提供する製品あるいはサービスの種類を増やしたり、事業プロセスのデジタル化を推進したり、クラウドサービスへの依存度が増加したり、海外市場での販売が増加したりすると、サプライチェーンがより複雑化するかもしれません。その結果、貴社は、サイバー脅威の増加による複雑で途方もない対応を迫られることになります。情報セキュリティ監査は、無意味な文書化や透明性の欠如等により対応が難しいそのような状況に対して信用を強化するものであるべきです。

第1線での管理の困難さが 増大している

サプライチェーンの複雑化のみならず、それを支えるにはプロセスとITシステムの利活用が増加します。定期的な認定管理、年次監査報告書、事件・事故の通知などを実施するには、複雑なスキルセットが必要です。

これらの法律、経営、技術に関する知識、しばしば言語スキルや能力が要求される実務を遂行していくのは容易ではありません。

- 人件費削減目的で選択的に外注を活用している中での、これらのスキルの完全な内製化は容易ではない。
- 適切なスキルと能力を持った人材がいるが、取引先リスクを取り扱う部門とは異なる部門に所属している。
- 適切なスキルと能力を持った人材がいるが、既存業務の負担が重く活用できない。
- 取引先等を管理する手続きが自動化されていない（当該分野へのIT投資が十分に行われていないため）。

Challenges – operational management view

Increasing complexity of the supply chain

The complexity of your supply chain increases along with the growth of your product / service portfolio, with your digital transformation, with the intensive use of cloud services and with a growing presence in overseas markets.

As a result, you have to keep a complicated, incomprehensible „array” secure from growing cybersecurity threats.

Information security assurance should reinforce trust against this background, which often fails due to meaningless documentation, lack of transparency and the time disadvantage of your cyber defence.

1st-line controls get harder

Not just the complexity of the supply chains, but also that of the underlying processes and IT systems is increasing. The regular control of the related certifications, yearly audit reports, incident notifications etc. also requires a complex skillset.

These legal, management, technical and often language skills and competences are often unavailable at the operational level:

- The internal establishment of these skills and competences was never even set as an objective, as the outsourcing took place (among others) with the aim of reducing the associated human resource costs
- The skills and competences are available, but at a different organizational unit, than the one handling provider risks
- The skills and competences are available, but the relevant resources are overloaded
- There is a lack of automation regarding third-party control procedures, due to a low level of investment in this field

まとめ



情報セキュリティリスクへの対応は、サプライチェーン全体に対して行われるべきである。



情報セキュリティ監査は、サプライチェーンや法令による要請事項が増える中で重要な役割を果たす。



効果的な保証のための資格要件と管理の枠組みの確立、情報セキュリティリスクに関する賢明な意思決定は、当局が、経営者の個人的な責任を考える上での重要な要素となってきた。



情報セキュリティに関する認定の取得、取引業者の認定および監査報告書の定期的な管理は、経営レベルおよび実務レベル双方において、より大きな課題となっている。

Summary



The handling of information security risks should cover the complete supply chain.



Information security assurance plays a major role in this field, due to the increasing complexity of regulatory requirements and supply chains.



The establishment of the prerequisites for an effective assurance and control framework, and the prudent information security risk decisions are increasingly conceived by regulators as a personal liability of the senior management.



The acquisition of information security certifications, and the regular control of supplier certifications and assurance reports is becoming an ever greater challenge both at the management and at the operational level.

Contact/ コンタクト



Masashi Nomura/
野村 雅士

Director,
Japanese Desk/

ディレクター
ジャパングデスク

+48 604 496 342

mnomura1@kpmg.pl



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



kpmg.com/socialmedia

kpmg.hu

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Advisory Ltd., a Hungarian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.