ComplyCloud

NIS2

Done Right - and In Time

Your Speakers

Bas van de Meeberg

Marketing & Business Development Manager

vBoxx, The Netherlands

Almost 2 years of experiencing client cases

Jakob Krabbe Sørensen

Lead Legal Engineer

ComplyCloud, Denmark

+5 years of experience with IT law

Agenda

1. The rules
2. The solutions
3. Q&A

Agenda

1. **The rules**
   - What is NIS2?
   - Who is covered ?
   - What are the requirements?
   - What happens if you do not comply with the rules?
2. **Solutions**
3. **Q&A**

What is NIS2?

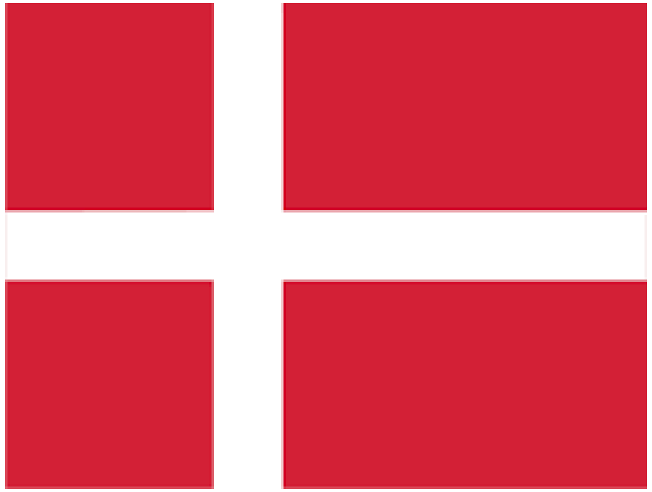
- **New EU Law on Network and Information Security (No. 2)**
- **The aim is to:**
  - improve cybersecurity across the EU and
  - align rules across the EU
- **It is a directive**
- **Must be implemented before 18. oktober 2024**

But…

Dilan says the Dutch rules will be delayed

And…

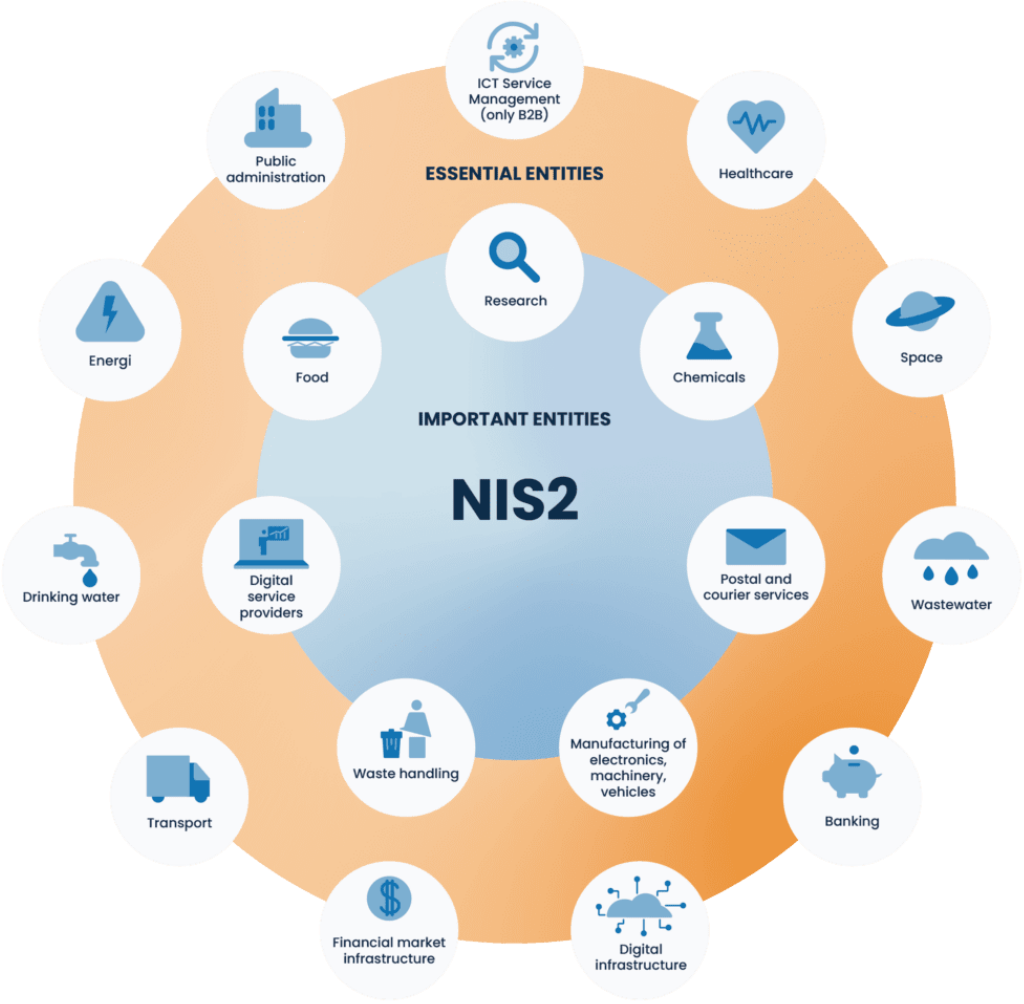
Troels says the Danish rules will be delayed



Who is covered? (at least)

All organizations that is:

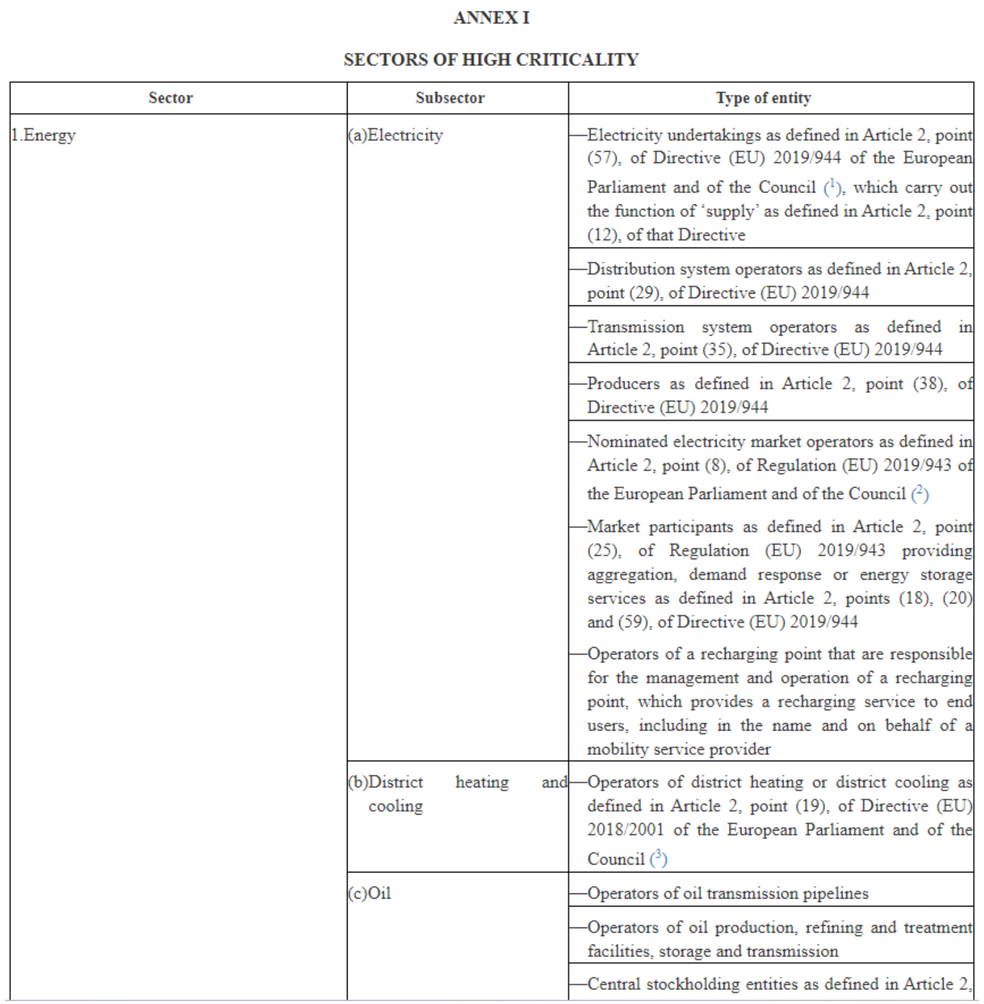
1. Operating in the EU
2. Medium-sized or larger
   - + 49 employees and
   - + EUR 10 million turnover and/or
   - + EUR 10 million balance sheet total
3. Listed in annexes 1 or 2 of NIS2



ComplyCloud

Who is covered? (at least)

An example:



ANNEX I

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1.Energy	(a)Electricity	—Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		—Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		—Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		—Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		—Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2]) —Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 —Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b)District heating and cooling	—Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c)Oil	—Operators of oil transmission pipelines
		—Operators of oil production, refining and treatment facilities, storage and transmission
		—Central stockholding entities as defined in Article 2,

Who is covered? (regardless of size)

No.	My own understanding	Description in the law
2	Public communications networks and services	providers of public electronic communications networks or of publicly available electronic communications services
3	Trust service providers	trust service providers
4	Entities providing domain name registration services;	top-level domain name registries and domain name system service providers
5	The sole provider of an essential service	the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities
6	Public safety or public health	disruption of the service provided by the entity could have a significant impact on public safety, public security or public health
7	Systemic risk	disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact
8	Critical to sector	the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State
9	National governmental entities	the entity is a public administration entity of central government as defined by a Member State in accordance with national law
10	Defined as critical in the Critical Entities Resilience directive	entities identified as critical entities under Directive (EU) 2022/2557;
11	Municipalities Regions Educational institutions (if decided)	member States may provide that this Directive applies to: (i) public administration entities at local level, (ii) educational establishments, in particular where they carry out critical research activities - - - the entity is a public administration entity at regional level, as defined by a Member State in accordance with national law, which, following a risk-based assessment, provides services the disruption of which is likely to have a significant impact on critical societal or economic activities.

Who are not covered? (despite previous slides)

A. Public authorities within:

- National or public security
- Defense
- Law enforcement, including the prevention, investigation, detection and prosecution of criminal offences

B. If decided, certain parts of the rules can be exempted for:

- Other organizations that perform or provide services within the 3 points above

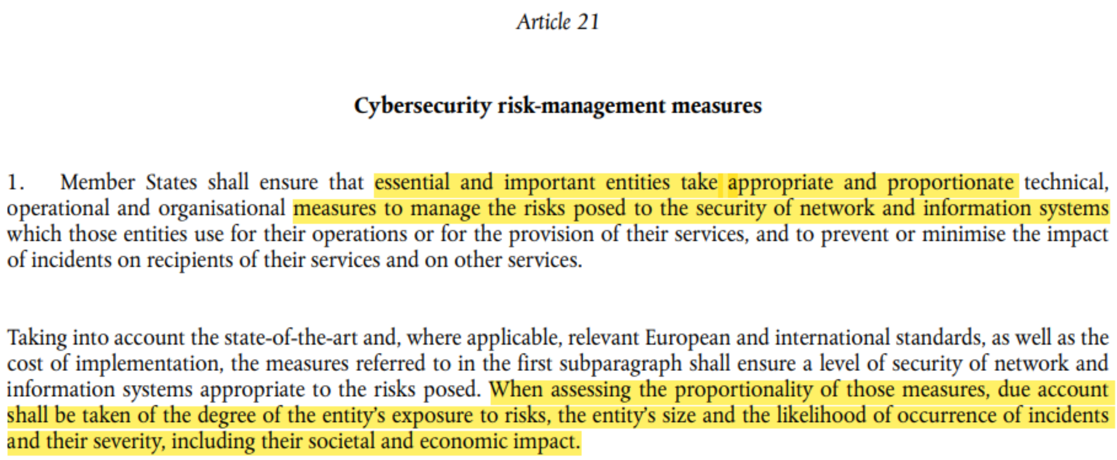
C. If the unit is exempted from regulation 2022/2554, cf. article 2, paragraph 4 (financial sector)

1. (in short: if covered by DORA, you must comply with both things, but DORA takes precedence)

What are the main rules?

1. Appropriate security + minimum requirements
2. Supply chain security
3. Obligations for the management
4. Training
5. Incident reporting
6. Sanctions, including fines

Appropriate security

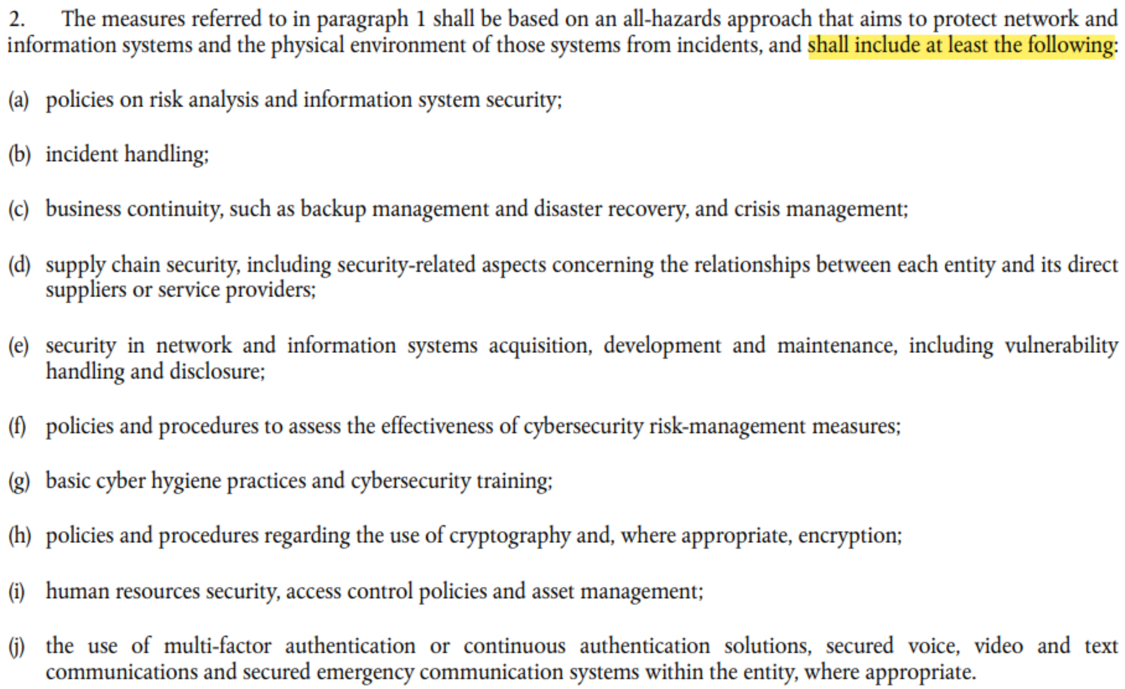


Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.



2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

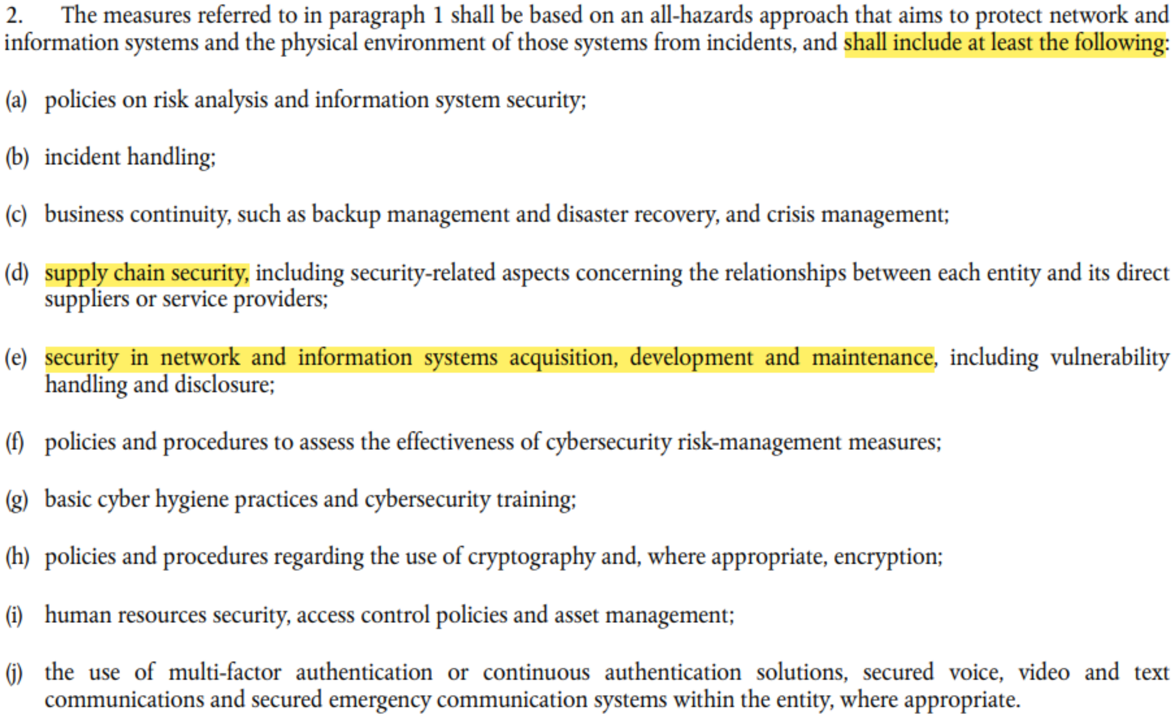
(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Supply chain security



2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

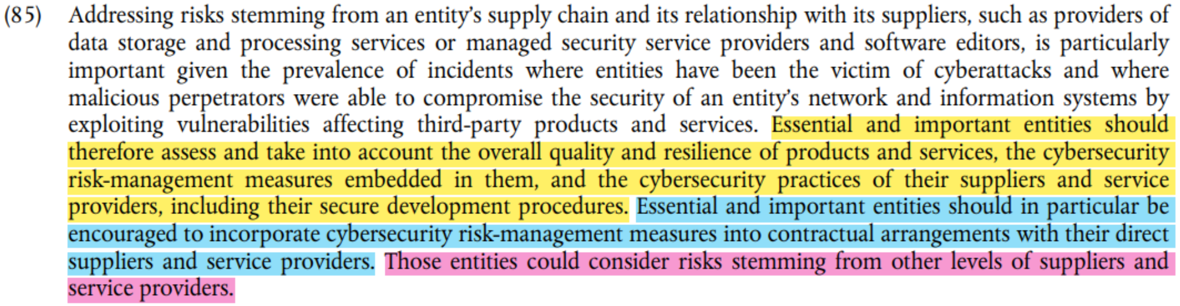
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

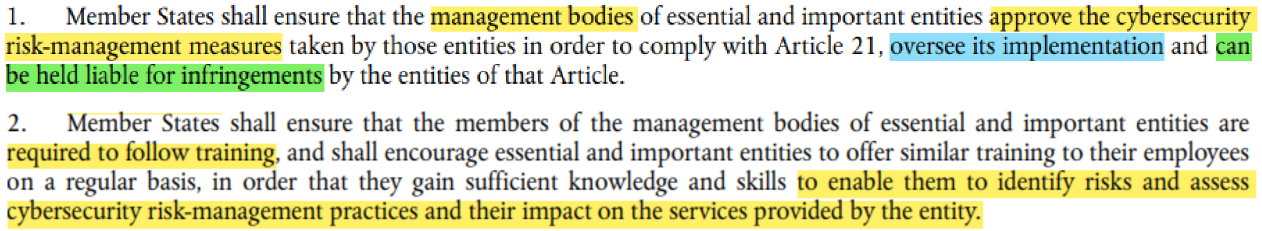


(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

ComplyCloud

Obligations for the management

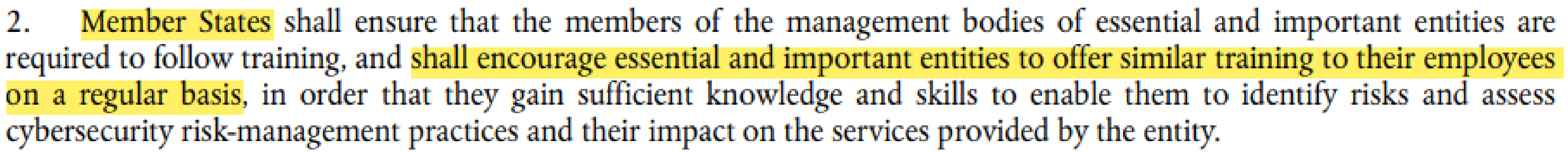
- **Approve the measures to manage cyber security risks**
- **Supervise their implementation**
- **Must follow courses**



1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

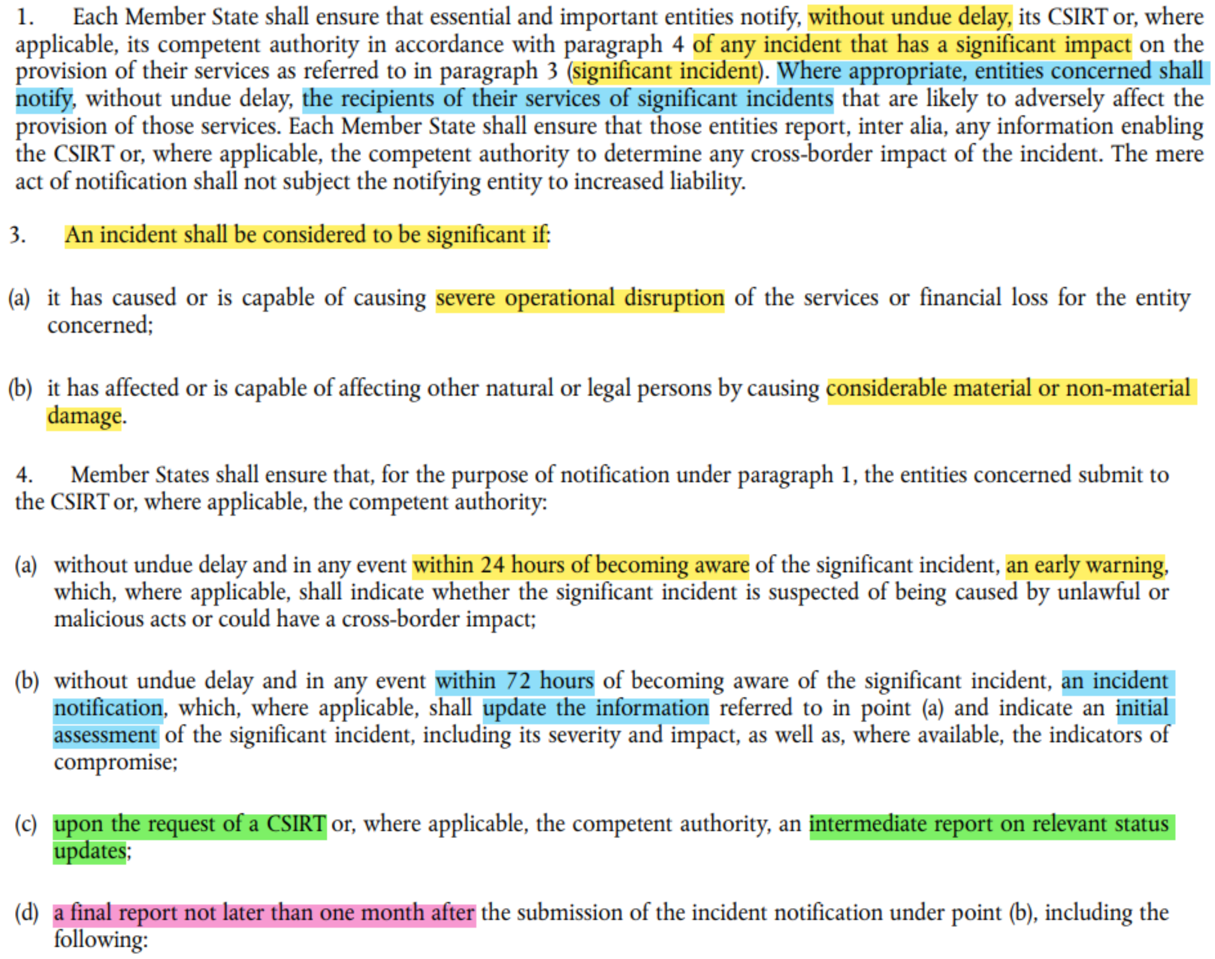
2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Training of employees (maybe)



2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Incident reporting



1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

3. An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

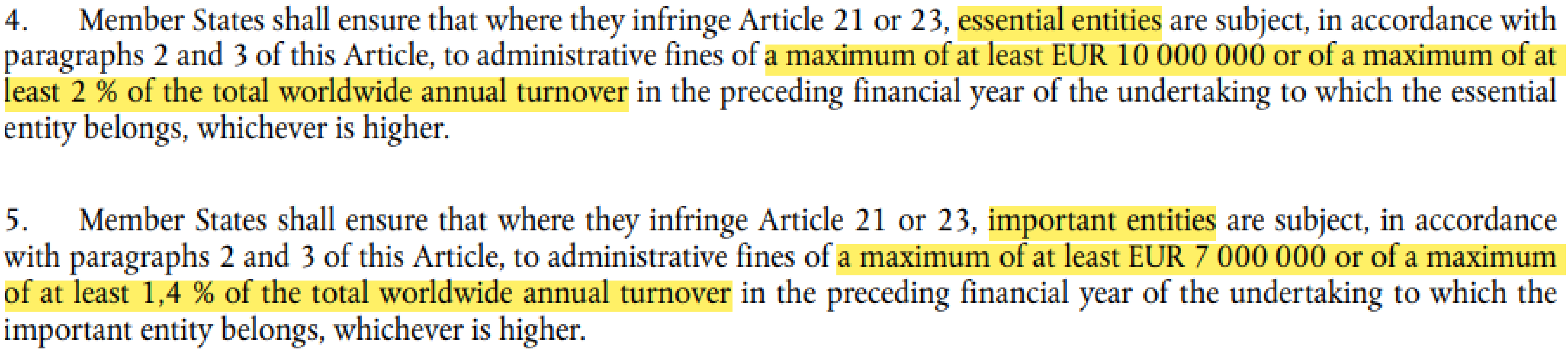
(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

Sanctions

The competent authorities can, as a minimum:

1. **Give warnings and binding instructions (incl. on compliance with Articles 21 and 23)**
2. **Require entities to notify those affected by a potential cyber threat or to make the threat/incident public**
3. **Appoint a monitoring officer to oversee the entity's compliance with Art. 21 and 23**
4. **In addition to above: Administrative fines (when there is practice for this -> otherwise like GDPR)**
5. **If the above is ineffective, the authorities can again request remedial action. If that does not work, the authorities can:**
   - To temporarily suspend a certification or approval of the device
   - Request the relevant bodies or courts to temporarily prohibit a person with management responsibilities from exercising management functions in the entity
6. **EU nationals must ensure that the responsible persons can be held accountable for breaching their obligations to ensure compliance with NIS2**
   - Applies to both essential and important units

Maximum penalties

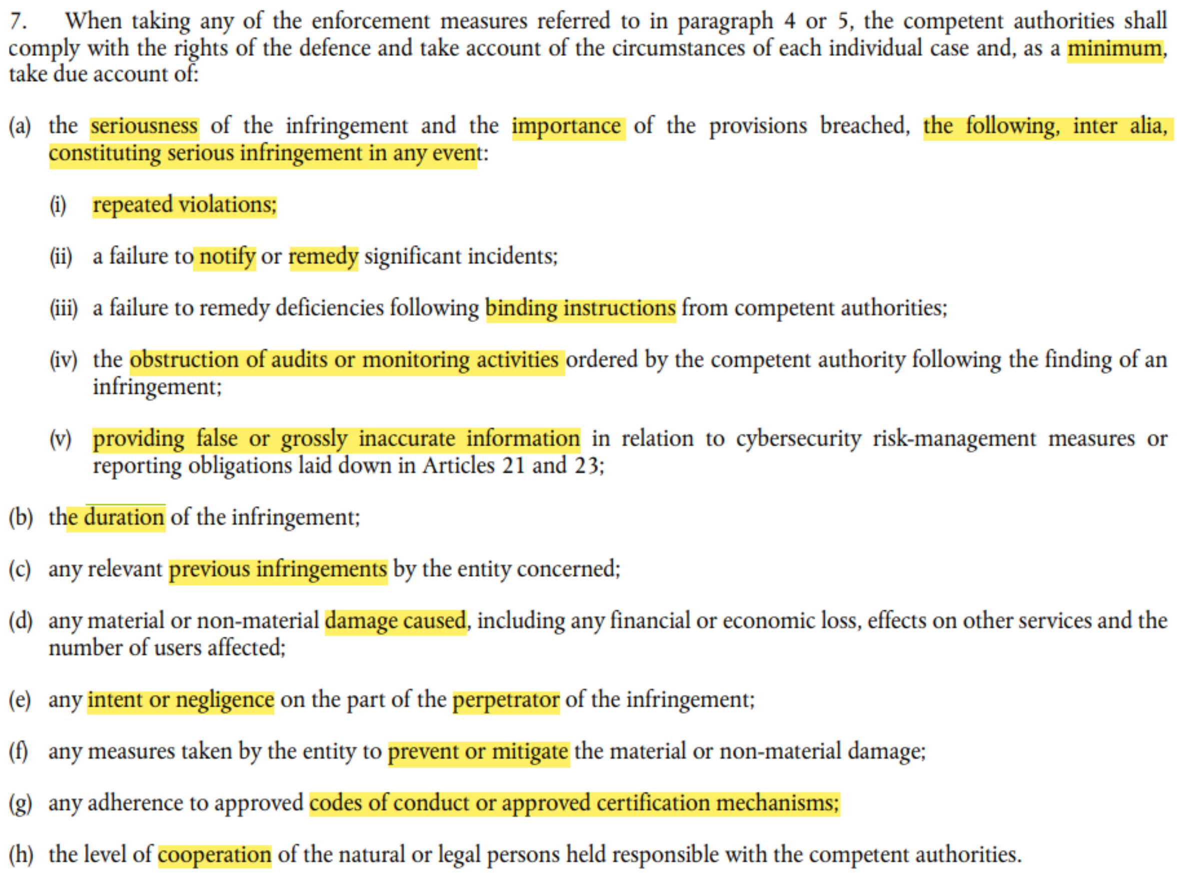


4. Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

5. Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

- **Court practice will probably say more about the actual size of the fine**

What will the sanction be based on?



7. When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:

(i) repeated violations;

(ii) a failure to notify or remedy significant incidents;

(iii) a failure to remedy deficiencies following binding instructions from competent authorities;

(iv) the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement;

(v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23;

(b) the duration of the infringement;

(c) any relevant previous infringements by the entity concerned;

(d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;

(e) any intent or negligence on the part of the perpetrator of the infringement;

(f) any measures taken by the entity to prevent or mitigate the material or non-material damage;

(g) any adherence to approved codes of conduct or approved certification mechanisms;

(h) the level of cooperation of the natural or legal persons held responsible with the competent authorities.

Agenda

1. The rules

2. Solutions

   - How does a NIS2 plan look?
   - Specific tools
   - Your path to NIS2-compliance
   - Importance of following your data
   - How to follow data
   - Example case and context

3. Q&A

What does a NIS2 plan look like?

1. **Assess: How much security do you need? (to protect "network and information systems")**
   - See e.g. ISO 270XX, NIST SP 800-X, CIS 18, ISA 62443-X etc.

2. **Remember: Include minimum requirements from NIS2**
   - Article 21 (2)
   - Courses for management and perhaps employees
   - Incident reporting
   - Extra national requirements

3. **Do: Implement and maintain security**

4. **Document: Remember to write it down**

Specific tools

- NIS2

- The directive (link)
- Rapport udarbejdet af IRIS GROUP for Industriens Fond (link)
- ENISA webpage (link)
- Report from ENISA about budget requirements for NIS (link)
- Analysis from the EU Commission about NIS 2 (link) – VERY LONG
- NIS2 quickscan tool from the dutch government (link)

- The ISO/IEC 27000-series

- Webpage (link)

- CIS Controls

- Webpage (link)

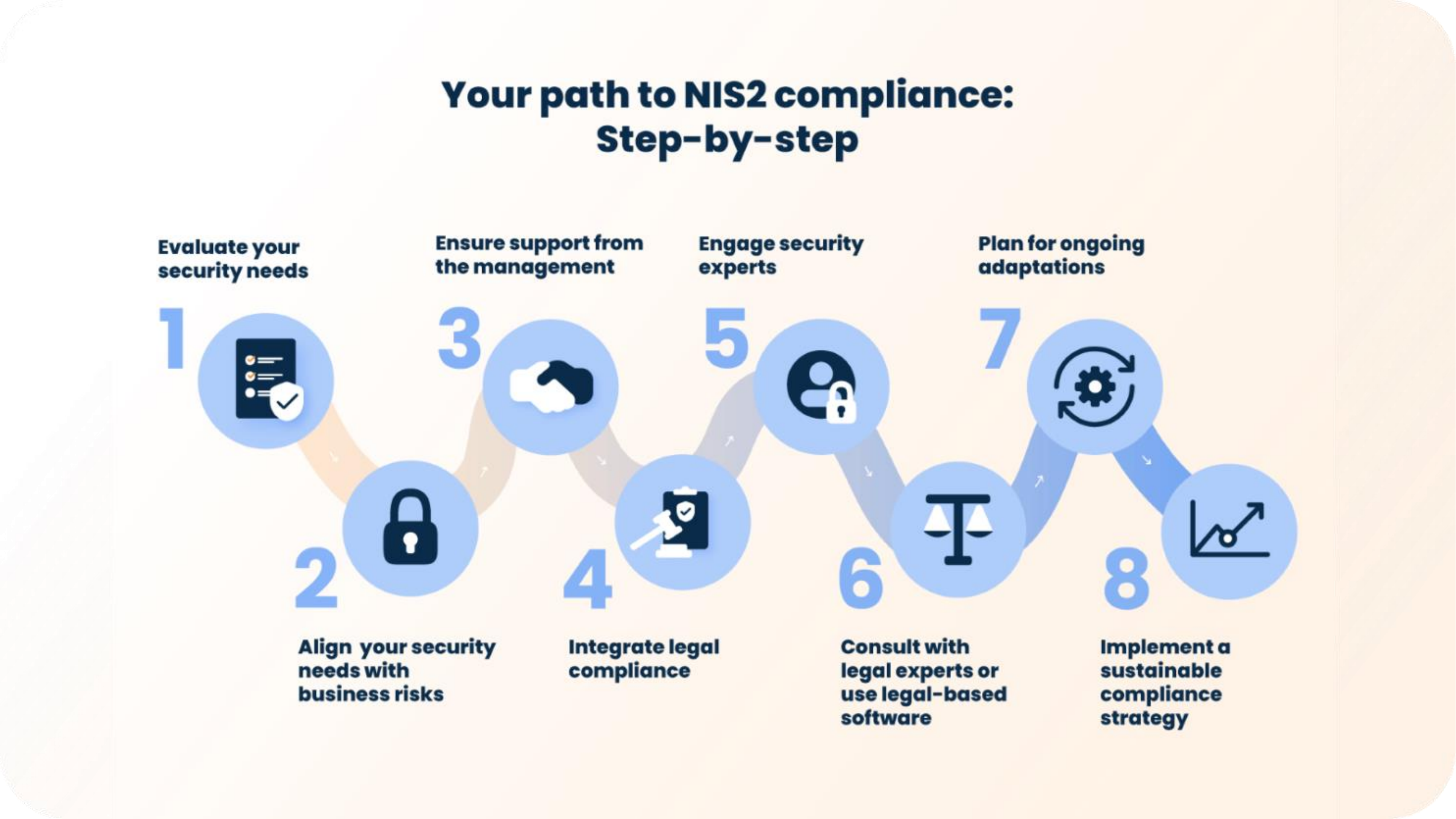
- ISA/IEC 62443-serien

- Introduction from International Society of Automation (link)

- NIST Cybersecurity Framework

- Webpage (link)
- Standard (link)
- + NIST SP 800-53 for controls (link)

Rollout: Your way to NIS2



Your path to NIS2 compliance: Step-by-step

1 Evaluate your security needs

2 Align your security needs with business risks

3 Ensure support from the management

4 Integrate legal compliance

5 Engage security experts

6 Consult with legal experts or use legal-based software

7 Plan for ongoing adaptations

8 Implement a sustainable compliance strategy

Why ComplyCloud?

What do we provide:

- A software solution that provides the right and necessary NIS2 documentation
- An expert team giving peace of mind from implementation to legal support and automated tasks
- Training for management and employees

Features overall:

- Easy interface in questionnaires to create documentation
- Creation of legally correct documents with a huge time saving
- Automated controls and supplier audits
- Automated updating of documents when new case law or guidance occur
- Integration between GDPR, IT security and NIS2

Key points

1. We are still waiting for **national rules**.... and probably will for a while
2. Some companies will be **directly covered** by the rules, and others will be **indirectly affected** by them
3. We already know some **minimum requirements** that you can start looking into, including supply chain security
4. In case of non-compliance, you can be subject to **a broad range of sanctions**
5. Reaching compliance requires going through **eight consecutive steps** in your organization

Q&A

FAQ

- ISO 27001 vs NIS2?
- Supplier to a covered entity?
- Enough resources?

What we are going to cover

- The importancee of following your data
- How you actually follow your data
- How to analyze your data chain
- Examples

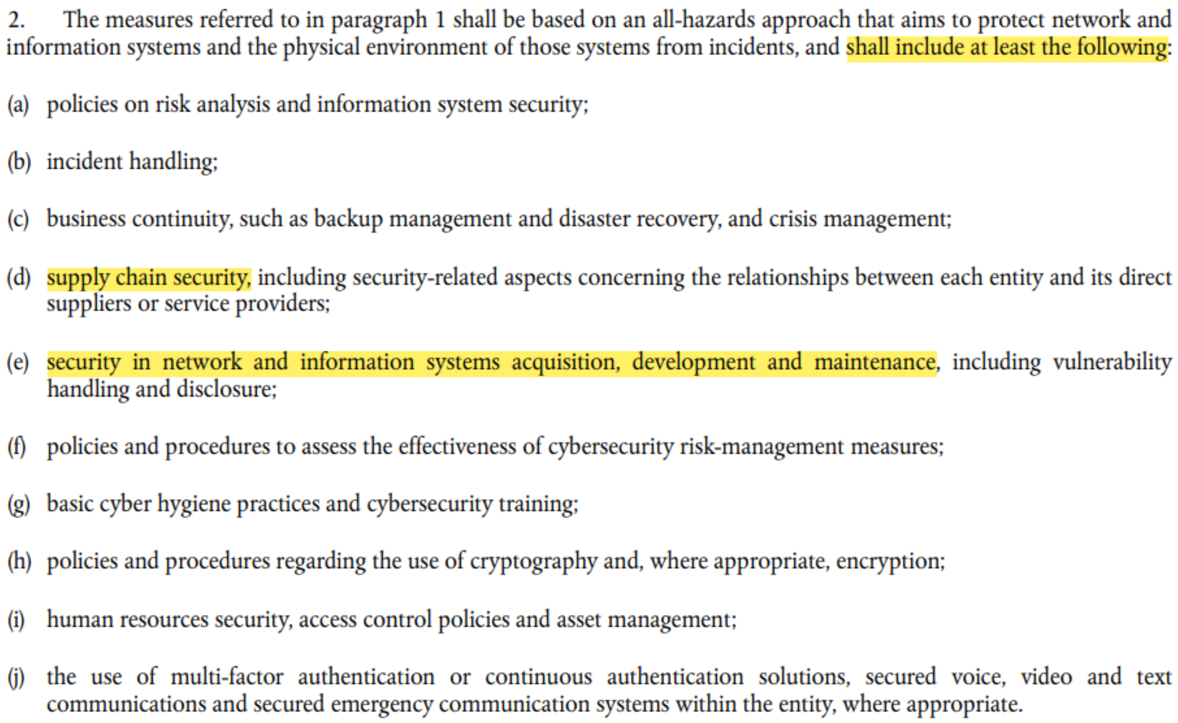
The importance of following data

- Data is a very valuable asset, so tracking it ensures it does not end up somewhere you don't want it to

- NIS2 is not just about checking boxes. You need to know how data moves to really understand.

The importance of following data

- **NIS2 is not just about checking boxes. Let's not forget the requirements discussed earlier:**



2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

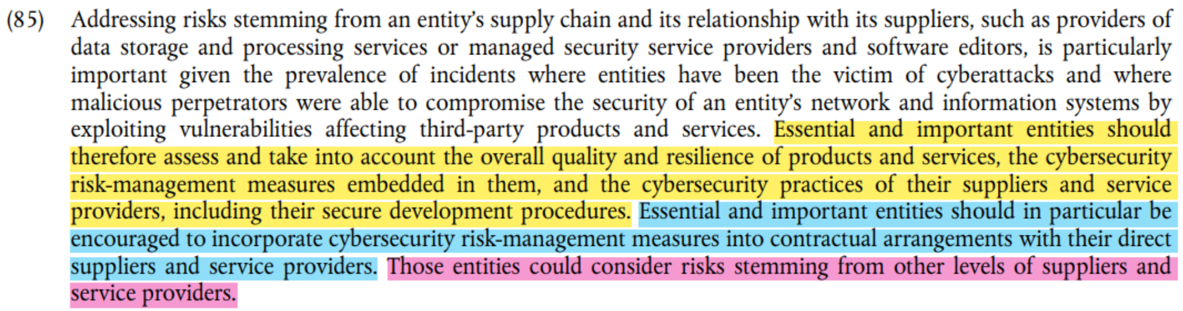
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.



(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

The importance of following data

- Data is a very valuable asset, so tracking it ensures it does not end up somewhere you don't want it to
- NIS2 is not just about checking boxes. You need to know how data moves to really understand.
- Your business might handle data securely and you possibly even have a certification like ISO 27001. However, what happens when data leaves your control?

The importance of following data

- **It allows you to:**
  - Know that your defense against cyber attacks is handled correctly
  - Minimize risks
  - Build trust with your own customers

- **It can be quite challenging!**

- **Therefore, having a good system and strategy is key**

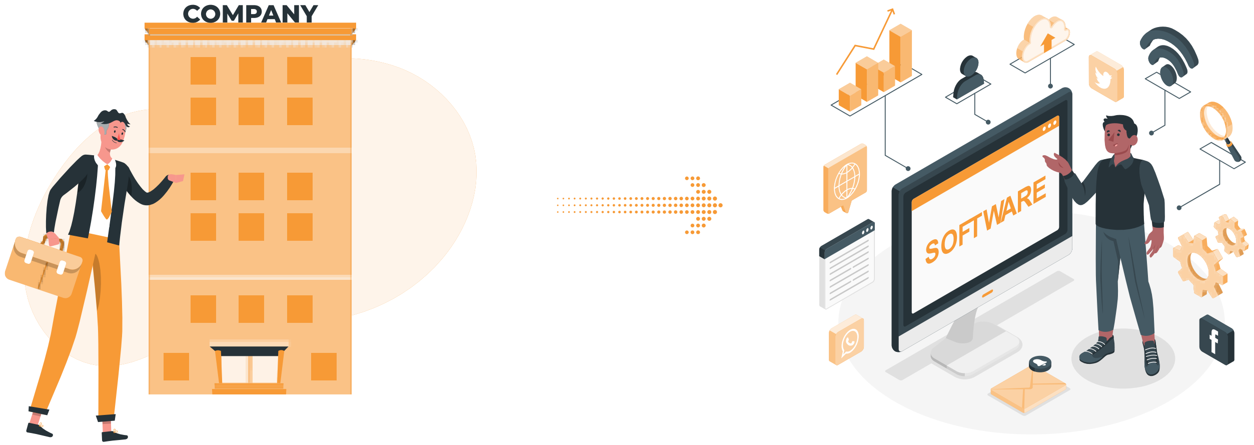
How to follow your data?

- It is crucial to understand data flow inside AND outside the company

- Map out what data you collect and why, where it is stored, how it moves from one place to another and who can get to it.

How to follow your data?

1. **Step 1: Your service providers**
   - ○ Ask the provider directly
   - ○ Look for processing agreements
   - ○ Look for privacy statements or subprocessor documents



How to follow your data?

1. Step 1: Your service providers
2. Step 2: Their subprocessors (and their subprocessors etc.)

COMPANY
SOFTWARE
€
?

How to follow your data?

- The more service providers and subprocessors, the harder it gets to follow your data, if not practically impossible

COMPANY
SOFTWARE
€
?

This is when data is out of your direct control

How to follow your data?

- **Data security is not just about protecting against hackers and such!**
- **Your service providers and subprocessors might be more detrimental to security:**
  - Microsoft and Google might be cost effective, but they do not make their money with the price of your subscription!
  - American company = no full data privacy As uncovered by the Dutch Intelligence & Security Service, published by NOS news: American government can read all emails under their Patriot/Cloud Act

vBoxx

How to follow your data?

- **Tracking Mechanisms**
  - Management tools
  - Access controls
  - Encrypting data

- **Keep reviewing**

- **Educate your teams**
  - Explain NIS2
  - Helps with spotting issues

Identifying subprocessors

- **Transparency challenges**
  - Included in service agreements
  - Might not be shared at all, or...
  - Even deliberately hidden

- **Be vigilant**
  - Insist on clear information
  - Other public sources or industry reports may help too
  - The goal is to put together a comprehensive list

Assessment of subprocessors

- **Security & Compliance**
  - In which country is data processed?
  - What are the laws in those countries?
  - Do they have certifications, like ISO 27001?

- **Engage!**
  - Might use questionnaires or audits
  - Opens up a line of communication
  - As said earlier: also document these interactions for compliance proof

Challenge example: Microsoft

- **Issues with transparency**
  - 47 subprocessors to assess and 36 datacenters
  - Very limited descriptions and explaination

- **Actually assessing is a nightmare**
  - Many companies outside EU and parent companies all over the world
  - Very limited documentation readily available from subprocessors

Developments

- **Shift in sentiment prompted by…**
  - Privacy and security concerns
  - A desire to simplify data security and monitoring

- **Simplifying means less work, better control and more security**

- **Think of the future**
  - What happens if the relationship between, for example, the EU and the United States deteriorates?
  - Current trends in legislation, like this NIS2 directive

Simplifying your data journey

- In short, many companies want to go from this:

Dozens of subprocessors in different countries and selling of data without any customer service or help

COMPANY
SOFTWARE
€
?

Simplifying your data journey

- **To this**
  - Fewer providers with more integrated services
  - Limit the amount of subprocessors
  - Fully EU hosted

Example case

- **Product quality is first criterium**

- **Privacy and security focused products are up to par or better than the previously popular solutions**

- **Not just a provider, but a partner**
  - Help with business cases
  - If something goes south, we are there

Why vBoxx?

- **Wide range of business and privacy-focused products:**
  - Cloud Storage and file collaboration (vBoxxCloud)
  - Email, calendar, and video calling (vBoxxConnect)
  - Password Management (vBoxxVault)
  - Other products like servers, webhosting, domain names and more…

- **All without subprocessors, ISO 27001 certified, transparent privacy policies, and data under your control**

- **We offer more than just products**
  - Help with your questions and free demos of our products
  - Speak to someone within 10 seconds
  - But most importantly: a partner that is there for you!
  - My email: bas@vboxx.nl or you can call to +31 70 206 0091

Key points

1. It is essential to track your data, but most importantly **understand your data journey**
2. Doing so improves your **defense** agains cyber attacks, allows you to **minimize risk**, and **build trust** with customers and partners alike
3. Can be quite challenging, so map out where your data goes. And remember to identify the **what, why, where, how, who**
4. Pay close attention to your service providers, but definitely do not forget subprocessors!
5. It is not only about the companies, but also about the location
6. Less processors = less work and risk

Q&A

vBoxx

ComplyCloud

Contact us

vboxx.eu
complycloud.com