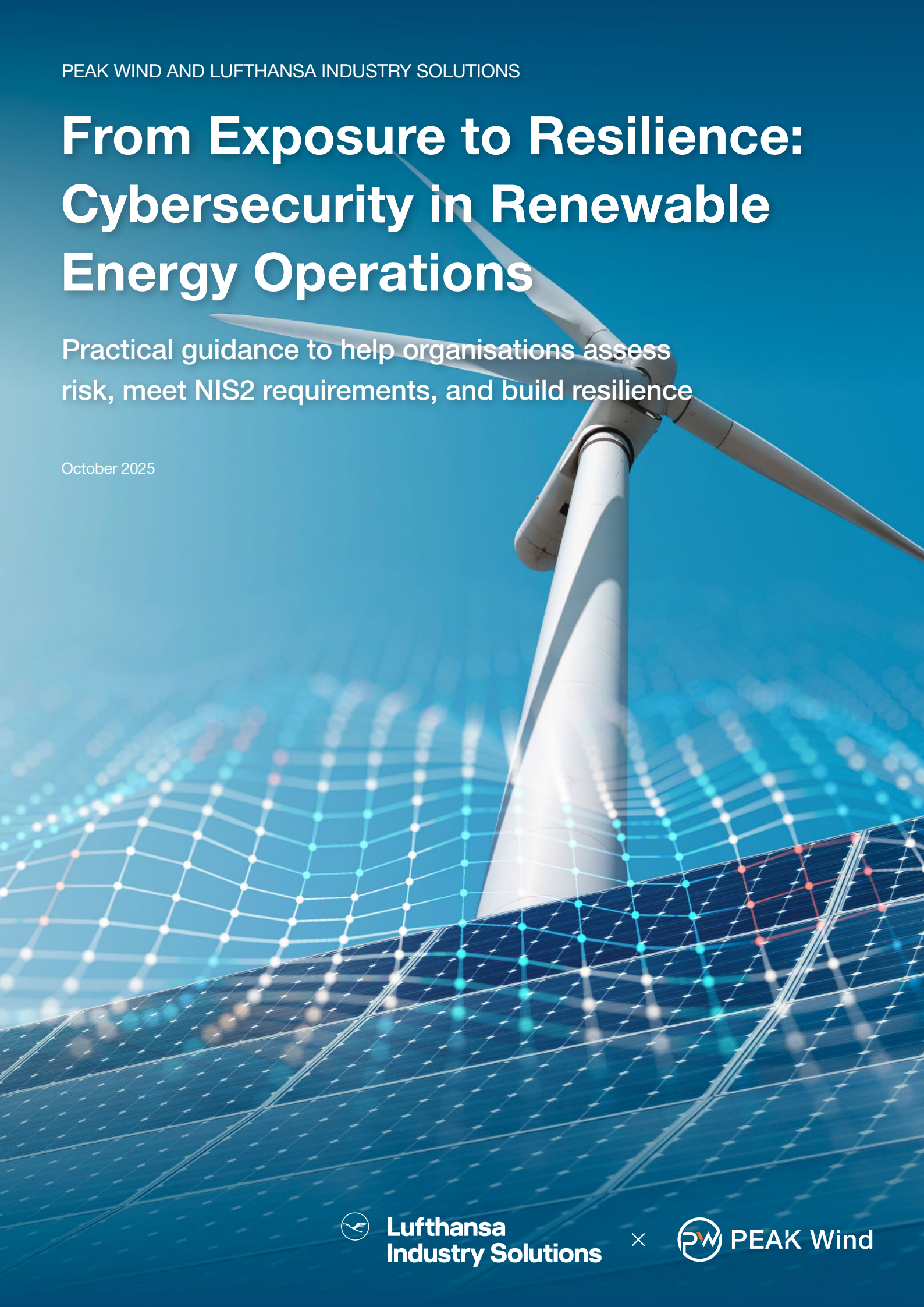
PEAK WIND AND LUFTHANSA INDUSTRY SOLUTIONS

From Exposure to Resilience: Cybersecurity in Renewable Energy Operations

Practical guidance to help organisations assess risk, meet NIS2 requirements, and build resilience

October 2025



Lufthansa Industry Solutions × PEAK Wind

Earlier this year, PEAK Wind and Lufthansa Industry Solutions published a joint article exploring two foundational cyber security questions organisations should ask themselves. The article provided practical examples and actionable steps to help renewable energy organisations better understand their current cyber security exposure and legal obligations.

In this whitepaper, we continue to explore the steps organisations could take and offer a holistic approach to managing cyber security risks, tailored specifically to the renewable energy sector.

In the first article, we discussed how to evaluate whether your metaphorical door is already open to vulnerabilities, and what you as an organisation are legally required to do, with a focus on the EU NIS21 directive.

While NIS2 came into effect in October 2024, most member states have yet to fully implement the legislation. This is not a time to rest on your laurels; rather, organisations should still take relevant steps, as national transition periods will be very short. Energy production is considered critical infrastructure under NIS2, and securing energy supply has become an even stronger focal point.

In this comprehensive whitepaper, we will discuss:

- ***What is my risk exposure?***
- ***What is the right level of risk exposure for my organisation?***
- ***How can I actively manage cyber risk in my organisation?***
- ***How should I react to a cyber security threat?***
- ***How can I stay up to date with requirements?***
- ***Do I have what I need to manage Cyber Security in my organisation?***

---

[1] NIS2 (2022) is a European Union directive that strengthens cybersecurity requirements for essential and important entities in critical sectors, including energy. It updates the original NIS Directive (2016) by expanding the scope of organisations covered, introducing stricter risk management and reporting obligations, and holding senior management accountable for cyber resilience. Compliance ensures organisations can prevent threats through proactive risk mitigation and respond effectively to incidents to maintain business continuity and enable recovery.

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

What is my risk exposure?

The NIS2 directive places emphasis on senior management as the ultimately responsible for cyber security risk management, requiring a top-down approach to understanding risk exposure and determining a risk strategy.

Risk exposure refers to the potential threats, vulnerabilities, and consequences that could impact your energy assets. In the context of NIS2 implementation, this involves assessing the likelihood and impact of cyber threats that could compromise operational reliability and resilience. In this regard, two perspectives should be considered:

- The external perspective reflects what a malicious actor, typically originating from outside your organisations boundaries and without deep insight into your technical landscape would focus on.

- The second is the internal view, which is relevant to preventing damages caused by insiders or attackers who have already gained access to your networks, whether intentionally or by mistake.

By law, at least the first perspective needs to be addressed, though it is strongly recommended to consider both.

When considering your risk exposure, you should distinguish between risks to your information technology (IT) environments and operational technology (OT) environments. Both are subject to cyber threats, but the risks and mitigation measures may vary.

IT environments are generally more exposed to external factors due to internet connectivity, while OT systems are usually more closed, although the number of OT systems connected to the internet is rapidly growing.

Risk evaluation also differs between the two. The guiding principle of IT security focuses on ensuring confidentiality (protection of data), integrity (ensuring data is not altered by others), and availability of systems, often referred to as CIA. In OT security, the focus is on ensuring availability (keeping systems online), integrity (for example, the functionality of sensors), and confidentiality (protection of sensitive information) in systems (AIC). In the most severe cases, an availability or integrity risk in the OT environment, such as a malfunctioning sensor, could even result in loss of life.

In renewable energy operations, risk exposure includes potential unauthorised access to control systems, disruptions of electricity production, data breaches, and ransomware attacks.

The growing integration of IoT devices, increased reliance on remote access, and dependence on digital systems in renewable energy heighten these risks, making cybersecurity a top priority. Additionally, regulatory non-compliance can result in significant penalties, reputational damage, and loss of stakeholder trust. Operators also need to consider external factors such as geopolitical tensions, supply chain vulnerabilities, and targeted attacks against critical infrastructure.

There are many ways to identify risks in your organisation. Some factors are system-driven (data, alarms, monitoring), while other risks may be exposed or even created through processes.

Finally, it is important to consider human-driven factors as well. There are many ways to track and understand these risks, one a simple way is to pose questions, evaluate different scenarios and consult with skilled colleagues. Examples of questions could be;

- What would happen to our business case/ability to produce power if system X were offline for one week?
- If you were an attacker and wanted to target us, how would you do it, and how difficult would it be?

Assessing your risk exposure means understanding the potential threats and uncertainties that could impact your assets. Awareness is an important first step toward secure operations. The next step is to make an informed decision about the appropriate level of risk exposure for your organisation.

What is the right level of risk exposure for my organisation?

Determining the right level of risk exposure for your asset or organisation requires balancing operational needs, regulatory compliance, security objectives, and cost.

Begin by identifying your organisation's critical assets and understanding their importance to operational continuity and safety. Because they are mission-critical, these assets require focused attention, but the rest of your environment must not be overlooked, especially if you have flat networks without proper segmentation.

Then, evaluate the potential threats and vulnerabilities which are specific to your renewable energy operations. Your evaluation or risk assessment should include differentiated levels of criticality, with all systems classified. In energy production, some systems are more critical and could potentially cause an immediate shutdown. These should be given a higher risk score, with mitigation measures prioritised compared to supporting systems that might only cause minor disruptions.

Next, assess the likelihood of the identified risks. Both impact and likelihood determine the effective risk level. Decide on your organisation's risk appetite by considering financial, reputational, and operational tolerances for disruption. Align this assessment with the requirements of the NIS2 regulation, which mandates active management of cybersecurity risks for critical infrastructure.

Implement risk mitigation measures proportional to the level of identified risks. This may involve technical controls, process improvements, or employee training. Each risk mitigation measure should be evaluated against its cost, operational impact, and level of risk reduction. Regularly review and update your risk assessments to adapt to evolving threats. Engaging in industry collaborations and adopting proven best practices can further refine your understanding and management of risk exposure.

Lastly, ensure that the leadership team is involved in setting and endorsing the risk exposure threshold, fostering organisation-wide accountability. It is critical that the management team understands the risks in order to make an informed decision about protection. This accountability and buy-in are essential to maintaining focus on mitigating cyber risks—after all, the success criterion for a cybersecurity lead is that there are no successful attacks and, therefore, no visible evidence of the need to continue investing.

Once you have a clear picture of your risk exposure and have evaluated what an acceptable risk level is for your organisation, you should take active steps to manage it. Mitigation steps should be a conscious decision rather than an unintended output from another process.

How can I actively manage risk in my organisation?

There are clear steps you can take to ensure you are actively managing risk in your organisation.

The first step is to establish an Information Security Management System (ISMS). This is a management system that combines organisational requirements communicated through policies with operational measures and procedures. The primary goals of an ISMS are to track the completeness and effectiveness of the organisation's security posture and to continuously adjust rules and measures in response to the evolving threat landscape.

The intention of an ISMS is not to create a complex system of rules and policies that only serve the purpose of passing an audit, but rather to build an efficient framework for managing and tracking your security exposure.

To actively manage cybersecurity risks in your organisation, start by conducting a comprehensive risk assessment to identify vulnerabilities and threats specific to your renewable energy assets as discussed in the previous section:

- Develop and implement a robust cybersecurity strategy that aligns with NIS2 regulatory requirements, focusing on risk prevention, detection, response and recovery. These strategies should include comprehensive and clear policies and processes.

- Ensure that all employees, from operational staff to management, are trained in cyber security best practices to reduce the likelihood of human error. While all staff are expected to receive awareness training, additional and scenario-based training is recommended for relevant individuals.

- Adopt industry-standard security measures such as network segmentation, encryption, and multi-factor authentication to protect critical systems.

- Frequently review access rights and establish access management based on the principle of least privilege.

- Regularly update and patch software to address known vulnerabilities promptly.

- Establish an incident response plan, with clearly defined roles and responsibilities, to ensure swift action in case of a breach, and test this plan through exercises!

- Monitor systems continuously with advanced tools to detect anomalies, leveraging threat intelligence to stay ahead of emerging risks.

- Collaborate with stakeholders and partners to enhance overall resilience by sharing insights and strategies.

- Conduct periodic audits and simulations to test the effectiveness of your cybersecurity measures and refine them as necessary.

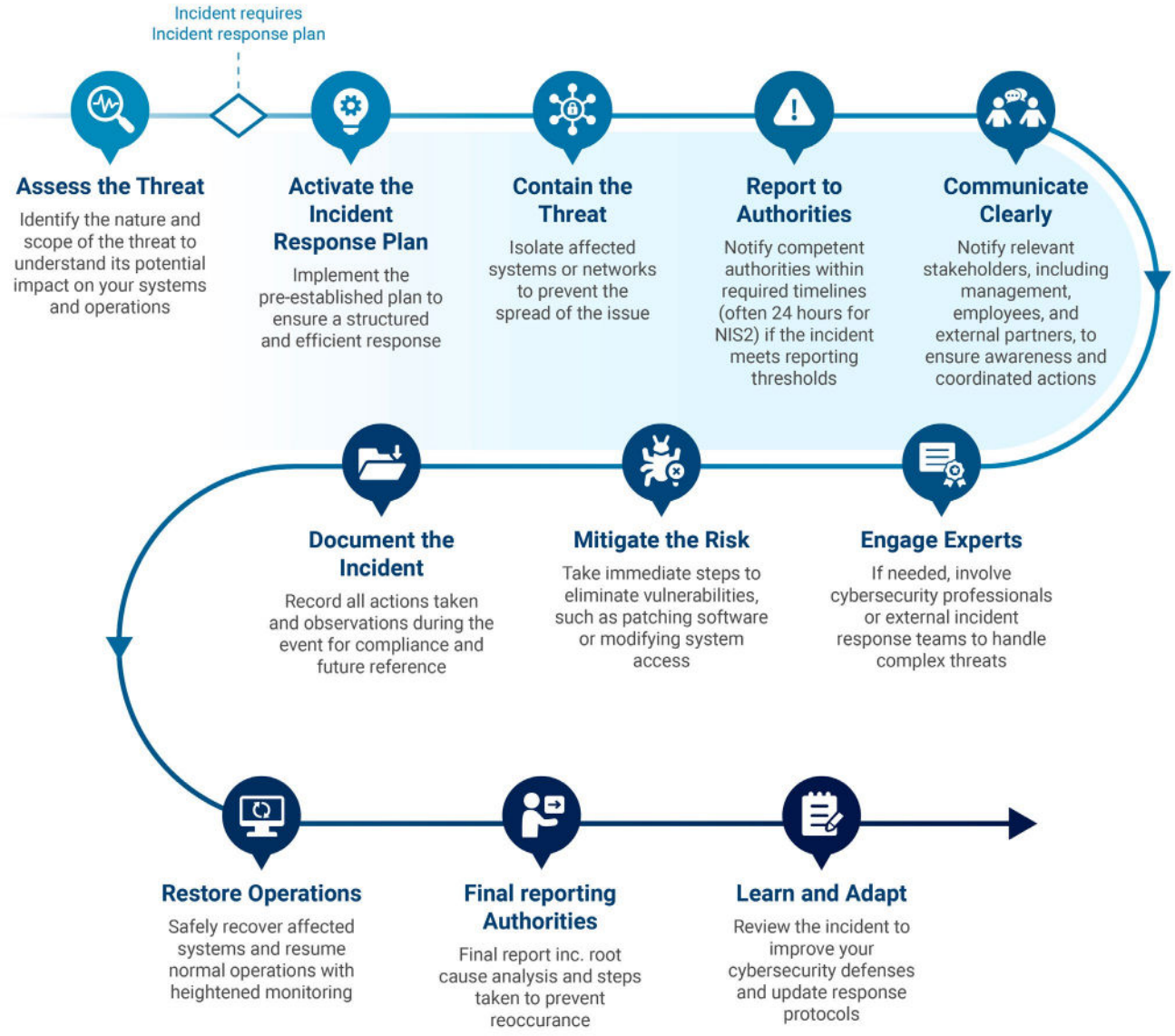
- Lastly, maintain a clear governance framework to ensure accountability and compliance across all levels of the organisation.

At this stage, you understand your risk exposure, have evaluated the acceptable level for your organisation, and have taken active steps to manage it—but how do you apply these measures when an actual threat is identified?

How should I react to a cyber security threat?

Cyber security threats will vary, and attackers are becoming increasingly cunning and dynamic in their methodology. Clear and established processes ensure efficiency and increase the likelihood of reducing the impact of potential threats. Individuals may react differently in situations, and the responses required for a minor, isolated system issue will differ from the response to a threat affecting the entire operating system. Awareness and regular practice of the steps internally will greatly improve your ability to handle actual threats.

When faced with a cyber security threat, recommended steps to take are:



Your initial step should always be to assess the alarm event to understand what actions to initiate. This can be partially automated for known patterns. In some cases, no further actions are needed, and the alarm is either resolved or deemed inconsequential. Otherwise, the next step is to activate the incident response plan, which should begin with classifying the incident. NIS2 Article 3(21) classifies a significant incident as *"one that has caused or is capable of causing severe operational disruptions of the services or financial loss". NIS2 takes a risk-based approach, allowing entities or national law makers to determine significance based on impact and severity.

Any incident for a renewable asset could be classified as:

Category	Impact
Critical	significant production loss, loss of control, breach of grid code
Major	partial production loss or error on critical systems
Minor	Minor effects on individual users, effect on non-critical systems

Once the incident response plan is initiated, all relevant individuals should be informed, including the authorities, at least in the case of critical incidents. The plan should contain clearly defined roles and responsibilities, as well as clear steps to be taken, outlining key decision points.

Phase 1: Detection and analysis

- Incident identification (reporter should provide clear information points: IT/OT assets affected, description of incident, name and contact details of the incident reporter)
- Classification – this should be a brief decision and can be re-evaluated continuously as more information arises.
- Notification of relevant stakeholders (including government authorities if required)
- Analyse the attack method and the attack behavior
- Start first isolation measures

Phase 2: Containment of threat

- Prevent further damage or data loss by containment measures. Can the incident be contained to a specific area or system?
- Activate workarounds for your operations if needed

Phase 3: Eradication and recovery

- Initiate disaster recovery if necessary
- If temporary workarounds have been used, ensure a permanent solution is implemented
- Confirm full operational recovery

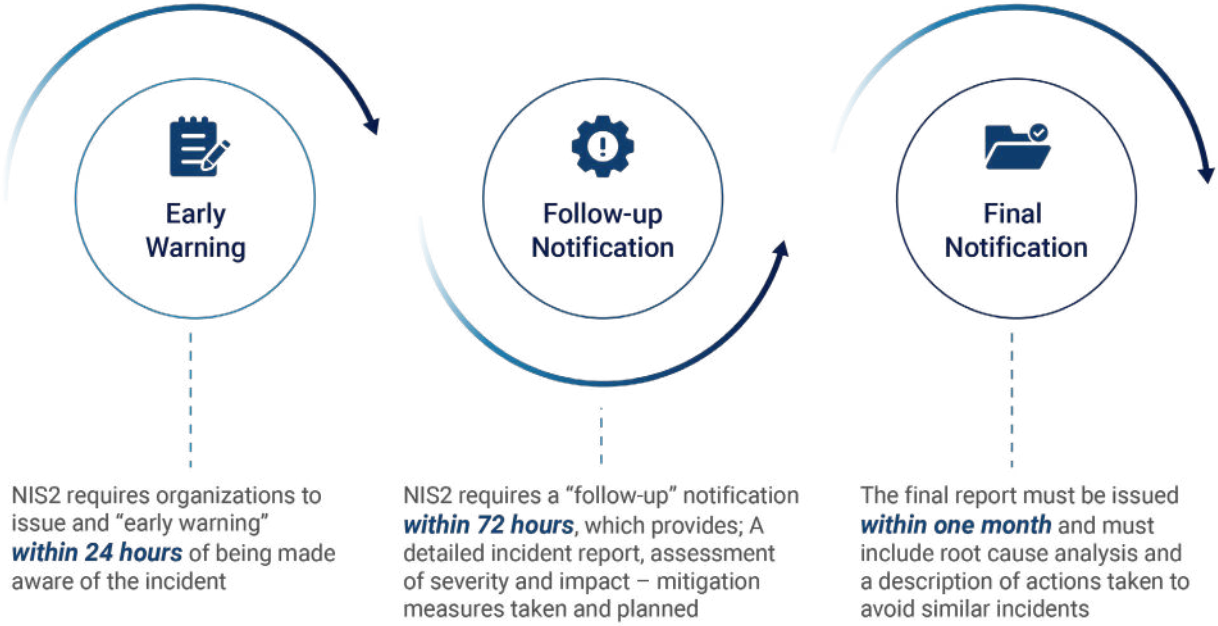
Phase 4: Post-incident activities

- Document the incident (incident report)
- Identify current risks (if any) and update the risk assessment
- Documentation of changes, if any, was made to resolve the incident
- Documentation of mitigation measures
- Capture lessons learned: can similar incidents be avoided in the future?
- Don't forget to submit the closing announcement for the authorities

* Source: European Union, EUR-Lex | https://eur-lex.europa.eu/eli/dir/2022/2555

Compliance requirements for incident reporting must also be considered and reflected in your processes. NIS2 requires significant incidents to be reported without undue delay and within 24 hours of discovery as a minimum. After 72 hours, the reporting body is required to provide a detailed report, and within one month, a final notification must be submitted outlining the steps taken to avoid recurrence and including a root cause analysis.containment measures. Can the incident be contained to a specific area or system?

NIS2 Incident Notification of National Authorities



While some steps will be the same across regions and assets, factors such as reporting to authorities, classification, and curtailment will vary. It is therefore important to consider these differences and ensure you are up to date with your specific requirements.

How can I stay up-to-date with requirements?

What should you do to make sure you are on top of on increasingly stringent and complex set of requirements?

We have proposed some practical steps to take. Navigating a complex compliance landscape can be daunting for any organisation, but understanding what is applicable to you is key. Renewable energy assets vary in production, grid contribution (sensitivity), size, regional impact, and financial impact. While NIS2 classifies energy production as critical, it is important to understand how your assets are classified and what requirements apply.

To stay up-to-date with NIS2 requirements, you should:

1. **Subscribe to official updates:**
   Regularly check updates from the European Union Agency for Cybersecurity (ENISA) and relevant regulatory bodies.

2. **Engage with industry forums:**
   Join renewable energy and cyber security associations where regulatory changes are discussed.

3. **Set up alerts:**
   Use keyword alerts on reliable news platforms or search engines to receive notifications about NIS2 developments.

4. **Attend conferences and webinars:**
   Participate in events focused on cybersecurity and regulatory compliance in renewable energy.

5. **Follow thought leaders:**
   Track insights from experts in cyber security and critical infrastructure on professional networks like LinkedIn.

6. **Invest in training:**
   Encourage your team to attend courses or certifications focused on NIS2 and cyber security frameworks.

7. **Collaborate with peers:**
   Share knowledge and experiences with other professionals in the renewable energy sector.

8. **Review periodic reports:**
   Read compliance and risk management reports from cyber security organisations.

9. **Use compliance tools:**
   Leverage software solutions designed to monitor and track regulatory changes in your industry.

10. **Consult legal and cyber security advisors:**
    Regularly consult experts to ensure your strategies align with current and upcoming requirements.

Above, we provided some practical steps to take, but staying up to date with requirements and legislation can at times be very complex.

Some organisations operate in multiple regions and have multiple subsidiaries where different legislation may apply. For example, US companies operating critical infrastructure in the EU will be required to perform a risk assessment to comply with NIS2.

You must ensure you know what is applicable to your organisation.

Do I have what I need to manage cyber security in my organisation?

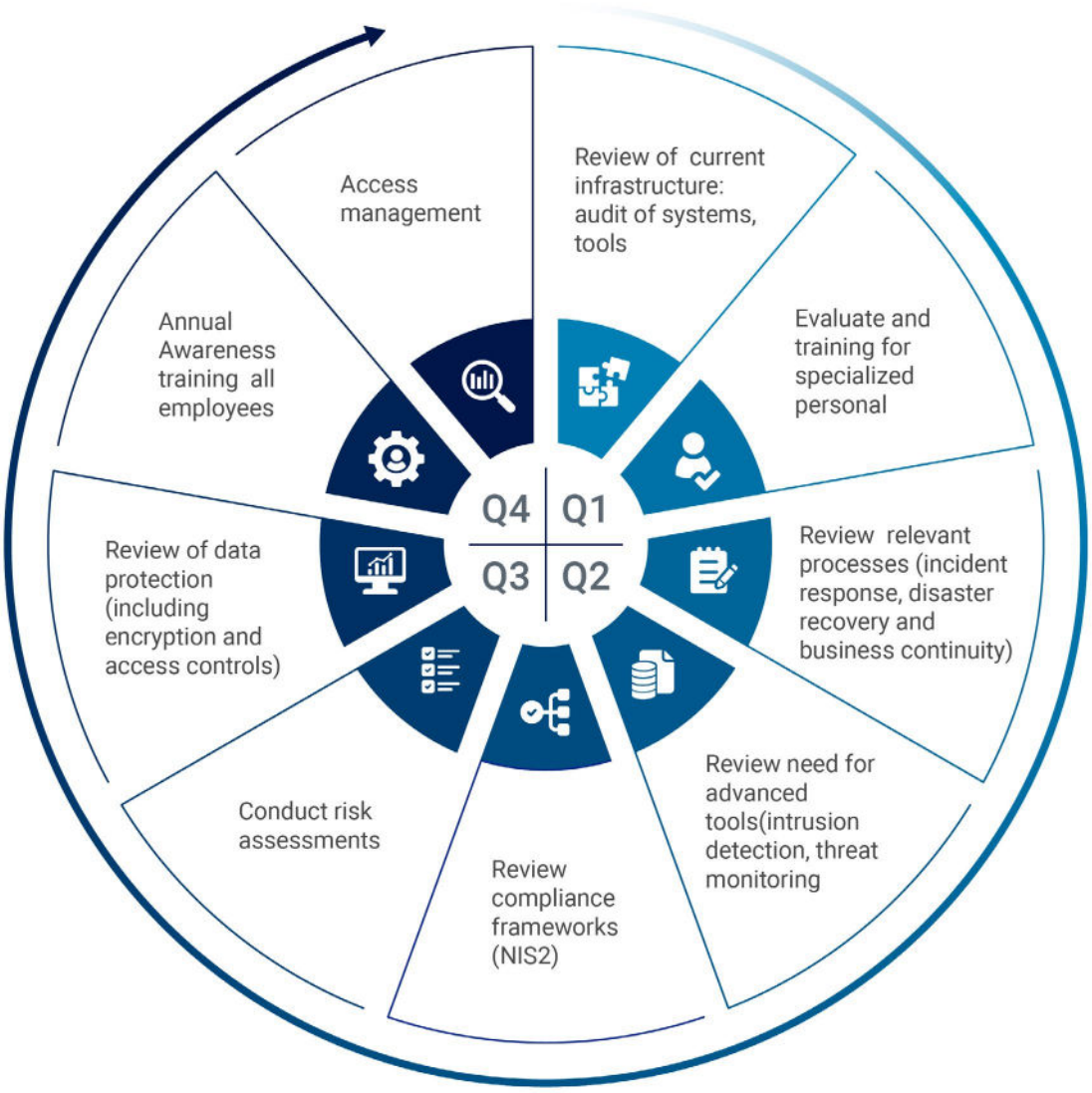
After defining an acceptable risk level in your organisation, you should evaluate which risk mitigations you may have in-house and which services make sense to outsource. Cyber security requires specialised knowledge and equipment. In some cases, it may not be practical for leaner organisations to manage this internally.

To determine if you have what you need to manage cyber security in your organisation, you should consider at least the following aspects

1. **Team's expertise:**
   - Ensure your personnel have the necessary skills
   - Train your employees to handle cybersecurity challenges
2. **Foster a cybersecurity culture:**
   Train your employees on cybersecurity best practices and promote awareness.
3. **Conduct risk assessments:**
   Regularly evaluate risks and vulnerabilities across your operations.
4. **Incident response planning:**
   Ensure you have a clear, tested plan to manage potential security breaches or disruptions
5. **Compliance with laws and frameworks:**
   - Verify which laws your organisation has to be compliant with (e.g. NIS2, CER, CRA, EU AI Act and GDPR)
   - Choose a suitable security governance framework (e.g. ISO 2700x, "IT-Grundschutz" by BSI or NIST CSF)
   - Ensure your documentation is practical and feasible for auditors
6. **Monitor for updates:**
   Stay informed about emerging threats and new regulations to maintain preparedness
7. **Prioritize data protection:**
   Implement measures to secure sensitive data, including encryption and access controls
8. **Engage external expertise:**
   Work with cyber security consultants or third-party vendors to complement in-house capabilities when needed

Once you have determined whether you have what is needed to manage cyber security in your organisation and addressed any shortcomings, it is important to establish an annual cycle to revisit all of the above.

Threats change, employees join and leave, and access management and risk assessments must be carried out regularly. Establishing a clear annual cycle allows you to maintain oversight and ensure you continue to have what you need to manage cyber security effectively.



Continuous alignment is key to staying secure and remaining economically efficient.

To extend capabilities and to raise efficiencies, we finally want to highlight useful security tool families, categorised after the NIS2 Cybersecurity Framework 2.0 scheme:

1. Identify

- Have an ISMS solution. It supports you in identifying your risks, managing your policies, controlling and tracking the risk mitigation progress
- Have an asset management solution and integrate asset discovery tools to keep it up to date

2. Protect

- Focus on your identity and access management solutions
- Use network segmentation and firewalls (perimeter + WAF) incl. a DDoS protection service
- Implement an attack surface management solution to check your own internet-exposed assets and those of partners and suppliers
- Use a vulnerability management solution that includes different sources, e.g. like vulnerability scanners, penetration tests, or bug bounty platforms
- Use software distribution solutions for your patch management

3. **Detect**
    - Use XDR solutions or services like EDR, NDR, SIEM and SOAR
    - For your cloud-based IT, integrate a CNAPP solution
    - Leverage threat intelligence services
4. **Respond**
    - Have your incident management procedures in a workflow solution
    - Conduct your investigations with proper forensic software and skilled personnel, or source this expertise from specialised vendors
5. **Recover**
    - Have a backup solution and test it (keep always offline backups!)

Awareness of what your organisation has available and where the gaps are is vital to evaluating risks and determining your organisation's risk strategy.

In this section, we have outlined methods and tools that you, as an organisation can deploy, as well as key considerations around their use.

Conclusions

In this whitepaper, we have discussed how your organisation can determine its risk exposure and what level of risk exposure is right for you.

We have outlined high-level steps to take if your organisation is faced with a cyber or OT incident, including what an incident response plan could contain. In an ever-changing environment of threats and legislation, staying on top of relevant requirements can be challenging, so we have suggested some high-level steps to serve as the starting point for your compliance programme.

Finally, we have discussed how to determine whether you have what is needed to manage OT and cyber security, and what steps you should take.

So, what to do now?

- Organise a cross-functional workshop focused on understanding your organisation's maturity level.
- Focus on developing a Risk Governance Framework through a systematic review of current roles and responsibilities, reporting lines and frameworks and a gap analysis to identify key actions.

About the authors

Matti Scheu
Director at PEAK Wind

Matti Scheu has worked in offshore wind industry for 12 years and is a specialist in asset, operations, and risk management, project management, OPEX and O&M planning. You may contact him by email at msc@peak-wind.com

Saša Jevremovic
Principal MRO Solutions

Saša Jevremovic has been with Lufthansa Industry Solutions since 2015 and is Principal MRO Solutions. He is responsible for business development in the wind energy sector and brings extensive experience in expanding international markets for maintenance, service, and repair solutions

Maren Dolva
Head of SCADA & Cyber Security

Maren has worked in the renewable energy sector for 6 years, with expertise in OT cyber security, and has implemented OT Security Management Systems on several assets in line with international and national standards. You may contact her by email mdo@gmail.com.

Christian Garske
Business Director– IT-Security

Christian Garske has been with Lufthansa Industry Solutions since 2008 and is Business Director of IT Security & Privacy. He combines deep expertise in cybersecurity and risk management with practical experience in safeguarding global logistics, shipping, and energy operations

About Lufthansa Industry Solutions

Lufthansa Industry Solutions (LHIND) is a leading IT service provider and part of the Lufthansa Group. With over 25 years of experience, the company offers innovative solutions and services in the areas of AI, IT Security, Cloud, IoT, SAP and more. Extensive know-how and cross-industry expertise make LHIND a reliable partner for the digital transformation. Its customer base includes companies both within and outside the Lufthansa Group, as well as more than 300 companies in various lines of business. The company is based in Norderstedt and employs more than 2,600 members of staff at several branch offices in Germany, Albania, Switzerland and the USA.

About PEAK Wind

PEAK Wind is an independent renewable energy specialist in commercial, financial and technical operations delivering advisory, intelligence and asset management services for investors and developers around the world. Currently managing +2.6GW of renewable energy assets for our clients and driving projects throughout the energy lifecycle to optimise O&M and enhance asset performance. PEAK Wind are experienced in delivering end-to-end experience on SCADA operation, data management, and cybersecurity for renewable assets.


Lufthansa
Industry Solutions
×
PEAK Wind