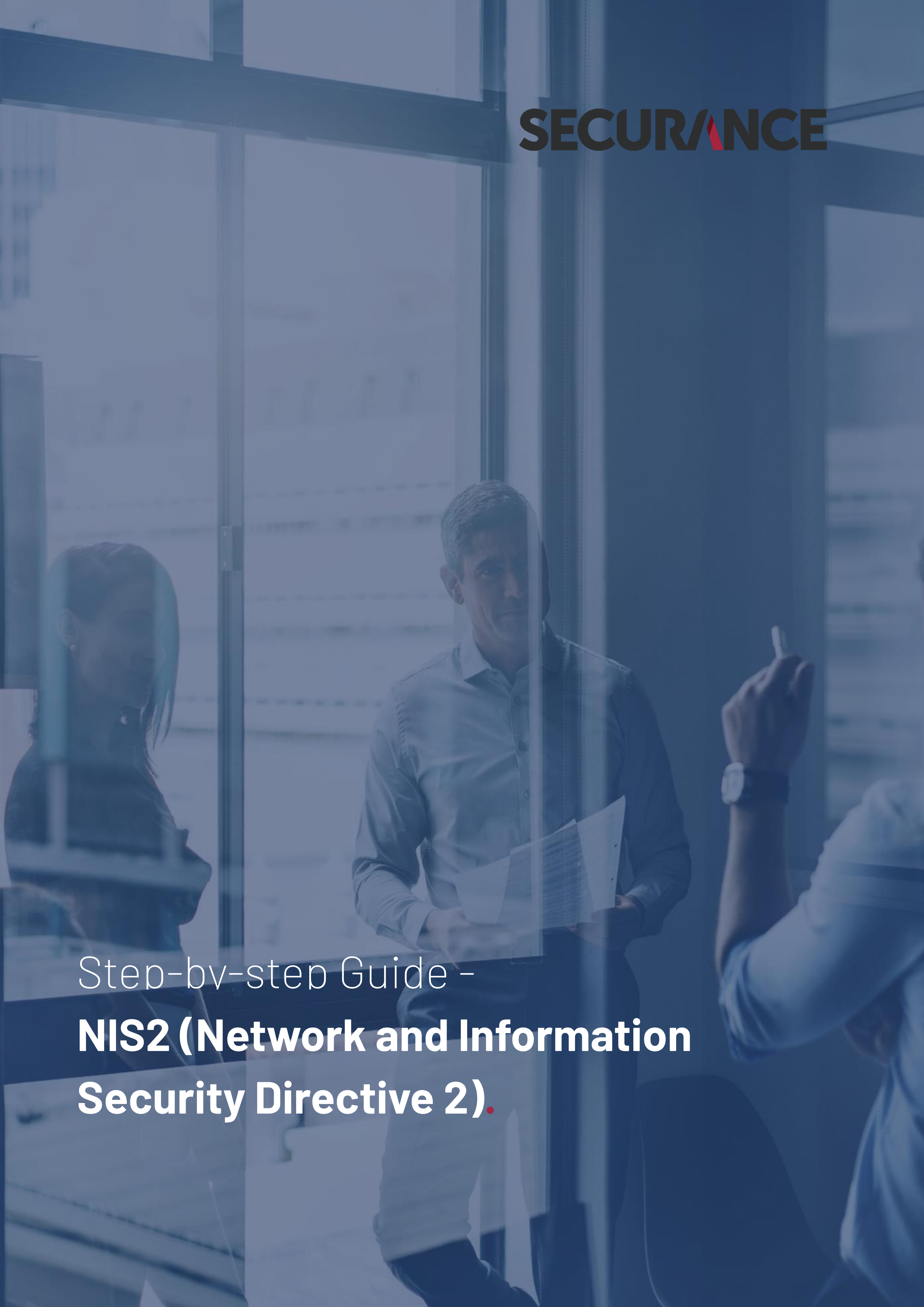

SECURANCE

Step-by-step Guide -

NIS2 (Network and Information Security Directive 2).

Introduction

The Network and Information Systems Directive 2 (NIS2) is a crucial regulation by the European Union aimed at bolstering the cybersecurity and resilience of critical infrastructure across various sectors. As a successor to the original NIS Directive, NIS2 introduces more stringent requirements and expanded coverage to enhance the security and continuity of essential and important entities within the digital landscape. Compliance with NIS2 is both a regulatory mandate and a vital strategy for organizations to safeguard their operations against an evolving array of cyber threats and disruptions.

This guide provides a comprehensive step-by-step approach for implementing NIS2 within your organization. We begin with the statement of applicability, detailing the specific NIS2 requirements pertinent to your entity. Following this, we conduct a gap analysis to pinpoint where your existing cybersecurity practices fall short of NIS2 standards. Based on this analysis, we develop a gap closure plan to address identified deficiencies. For medium and low priority gaps, we perform a detailed risk analysis to formulate effective mitigation strategies. Finally, we move to the implementation phase, where we execute the necessary measures to ensure compliance. By adhering to these steps, your organization can not only meet NIS2 requirements but also strengthen its overall resilience in the face of cyber threats and challenges.

NIS2

The primary objective of the NIS2 is to enhance the cybersecurity and operational resilience of essential and important entities across various sectors. This regulation mandates that organizations implement robust measures to manage and mitigate risks associated with network and information systems, ensuring their ability to respond effectively to and recover from cyber incidents. NIS2 extends its requirements to a broader range of sectors and entities, emphasizing the need for comprehensive cybersecurity practices and incident management.

The core components of NIS2 include:

- **Cybersecurity Risk Management:** Organizations are required to establish and maintain comprehensive cybersecurity risk management systems. This involves identifying, assessing, and mitigating risks related to network and information systems. Effective risk management includes having an up-to-date inventory of assets, assessing potential threats, and implementing measures to protect against identified risks.

- **Incident Reporting:** NIS2 stipulates that entities must develop standardized procedures for reporting significant cybersecurity incidents to national authorities. This requirement promotes transparency, facilitates prompt responses, and supports coordinated efforts among various stakeholders to address and mitigate the impact of cyber threats.

- **Resilience Testing:** Entities are required to conduct regular testing of their cybersecurity measures and systems to identify and address vulnerabilities. This includes performing vulnerability assessments, penetration testing, and other security exercises to ensure the robustness of their defences.

- **Supply Chain Security:** Recognizing the critical role of third-party providers, NIS2 mandates that organizations manage and secure their supply chains effectively. This involves implementing measures to assess and monitor the cybersecurity practices of external partners and ensuring that contractual arrangements address cybersecurity risks and responsibilities.

- **Operational Continuity:** Organizations must develop and maintain plans to ensure the continuity of their essential services, even in the face of significant disruptions. This includes creating and testing disaster recovery plans and business continuity procedures to ensure resilience in the event of a major incident.

By adhering to NIS2's requirements, organizations can significantly improve their ability to manage cybersecurity risks and ensure the continuity of their operations. NIS2 fosters a proactive approach to cybersecurity, encouraging continuous improvement and collaboration among entities, thereby strengthening the overall security posture and resilience of critical sectors.

Phase 1. Fit-Gap analysis level 1 and level 2

Identify which specific aspects of NIS2 apply to the organization

By conducting a thorough Statement of Applicability (STAP) analysis, the organization can clearly understand which NIS2 requirements are relevant to its operations and determine areas of compliance (FIT) and non-compliance (GAP). This analysis forms the basis for the subsequent steps in the compliance project, ensuring a focused and efficient approach to achieving full compliance with NIS2.

Actions:

- **Document existing compliance**
  Conduct an initial review of the organization's cybersecurity measures, policies, and procedures. Identify and document areas where the organization already meets NIS2 requirements, including existing risk management practices, incident reporting mechanisms, and security controls.

- **Identify and document gaps**
  Conduct a detailed review of NIS2 requirements and compare them against the organization's current state. Identify and document areas where the organization does not meet NIS2 requirements. This could involve missing policies, inadequate controls, or outdated procedures.

- **Evaluate impact and likelihood**
  Evaluate the priority of each identified gap based on its potential impact on the organization and the likelihood of exploitation.

  Consider the criticality of the affected systems and processes and the potential consequences of non-compliance. Divide the gaps into low, medium and high priority gaps.

- **Engage with stakeholders**
  Hold interviews with key stakeholders across different departments to gather detailed insights into current practices and to validate the identified gaps. Engage with IT, security, compliance, and operational teams to ensure comprehensive coverage of all relevant areas.

- **Review and validate**
  Conduct an internal review of the STAP analysis report with the project team and senior management to ensure its accuracy and comprehensiveness.

  Validate findings with relevant stakeholders to ensure alignment and buy-in.

- **Report and Feedback**
  A report summarizing the findings from the FitGap analysis will be compiled with a detailed descriptions of identified gaps and the current versus desired state for each. The findings will be presented to relevant stakeholders, and feedback will be gathered to refine the analysis.

Phase 2. Gap Closure Plan

Develop a comprehensive plan to address the identified gaps and achieve compliance with the NIS2

This step involves outlining specific actions for high-priority gaps and allocating resources to ensure that all compliance requirements are met effectively.

The Gap Closure Plan includes the following:

- **Analysis of both the current and desired situation**
  For each identified gap, the existing state of security measures and practices will be described as well as the desired situation. It includes detailing the specific deficiencies, how they fall short of NIS2 requirements and clear, measurable objectives that address the identified gaps.

- **Define specific actions and measures**
  For each identified gap, the actions required to bridge the gap will be specified. Details will include what needs to be done, who will be responsible, and the resources required.

- **Set priorities and timeline**
  The high-priority gaps will again be prioritized based on risk level, impact, and urgency. Also, a realistic timeline for each action will be developed, taking into account the complexity of tasks and availability of resources.

- **Implementation preparation**
  Comprehensive plans outlining the steps needed to execute each remediation action will be developed. This includes preparing any necessary documentation, training materials, and communication plans.

- **Document and report**
  A report summarizing the analysis, defined actions, priorities, timelines, and implementation preparations will be provided. The report will be presented to relevant stakeholders and is open to feedback to ensure all perspectives are considered. Potential first steps to kick-start the implementation of the actions mentioned in the gap closure plan will be included.

By following these steps, the organization can ensure a systematic and effective approach to closing identified gaps and achieving compliance with NIS2.

Phase 3. Risk Analysis for medium and low priority GAPs

Assess the risks associated with the identified gaps and prioritize actions

This step involves conducting a thorough risk assessment to understand potential threats and vulnerabilities of the identified low and medium priority gap

Actions:

- **Conduct risk analysis**
  The severity of each risk will be assessed by considering both its potential impact on the organization and the likelihood of its occurrence. Qualitative and quantitative methods will be used to evaluate these risks.

- **Assess impact and likelihood**
  The potential consequences of each risk on the organization will be determined. High-impact risks might include significant financial losses, severe reputational damage, regulatory fines, or major operational disruptions.

  The probability of each risk occurring will be evaluated. Factors influencing likelihood may include the organization's current controls, historical incidents, industry trends, and vulnerability to specific threats.

- **Create a Risk Matrix**
  A risk matrix that plots the likelihood of each risk against its potential impact will be developed. This visual tool helps categorize risks into different levels of severity. Based on the matrix, each risk will be categorized into appropriate levels. High-impact and high-likelihood risks will be prioritized as critical, while lower-impact and lower-likelihood risks may be categorized as low priority.

- **Develop a priority list**
  A prioritized list of risks based on their severity levels from the risk matrix will be developed. The focus will be on addressing the most critical risks first to mitigate the highest potential impacts on the organization.

- **Action planning**
  For each prioritized risk, specific actions and measures will be outlined. This might include enhancing security controls, updating policies, implementing new technologies, or conducting additional training.

- **Develop timeline**
  Realistic timelines for implementing the risk mitigation actions will be established. Actions that address critical risks with the highest impact and likelihood will be prioritized.

- **Documentation and reporting**
  Detailed records of all risk assessments will be kept, including the rationale for impact and likelihood ratings and the prioritization decisions.

By following these steps, the organization can effectively assess and prioritize the risks associated with the identified gaps, ensuring that resources are focused on the most critical areas.

Phase 4. Implementation

Implementing the actions

This step ensures that resources are allocated efficiently, focusing on the most critical areas to mitigate significant risks first.

Actions:

- **Execution of Gap Closure Plan**
  The specific actions to address the gaps identified during the FitGap Analysis will be implemented. These actions could include updating policies and procedures, enhancing technology infrastructure, implementing new security measures, or improving operational processes.

- **Communicating policy and process changes**
  Changes in policies, procedures, or practices will be communicated to relevant stakeholders within the organization. This ensures that everyone understands their roles and responsibilities in compliance with NIS2 requirements.

- **Testing and validation**
  NIS2 compliance measures typically involve testing systems and processes to ensure they work as intended.

- **Monitoring and Reporting**
  Mechanisms to monitor ongoing compliance with NIS2 requirements will be established. This could involve setting up regular audits, assessments, or continuous monitoring systems to detect and address any deviations or issues promptly.

- **Documentation and Reporting**
  Comprehensive documentation of all implemented measures, changes, and compliance activities will be maintained. This documentation is essential for demonstrating compliance during regulatory audits or inquiries.

- **Review and Continuous Improvement**
  The implemented measures will be periodically reviewed to assess their effectiveness and identify areas for improvement. Continuous improvement ensures that the organization remains resilient to digital operational risks over time.

- **Adaptation to Evolving Requirements**
  Given the dynamic nature of regulatory requirements, staying updated with any changes or updates to NIS2 and adapting the implementation plan accordingly will be ensured.

By following a structured approach to implementation, organizations can enhance their cybersecurity posture and ensure compliance with NIS2 requirements effectively.

Contact

Looking to promptly comply with the NIS2?

Our handy quick guide offers a straightforward, step-by-step approach to achieving compliance. Our expert team is ready to guide you through the four phases of this approach, from conducting an analysis to implementing operational improvements. All of this is done while incorporating our best practices and using our templates. Let us assist you in strengthening your network and information security and preparing your business for the future.

Contact us today at the number below for further clarification, consultation, and/or a quote for support, ensuring you're well-supported and confident in achieving NIS2 compliance.

Securance

63-66 Hatton Garden

London EC1N 8LE, UK

+44 20 351 446 56

www.securance.co.uk

Securance BV

Reactorweg 47

3542 AD Utrecht

+31 (0)30 2800888

www.securance.nl

Securance Sweden

Sidenvävargatan 17

753 19 Uppsala

+46703040656

Securance Germany

Josef-Orlopp-Straße 54

10365 Berlin

+4930439716860

BECOME THE ARCHITECT OF YOUR FUTURE

SECURANCE

Office The Netherlands
Address: Reactorweg 47 (4th floor)
3542 AD Utrecht, The Netherlands
Tel: +31(0)30 280 08 88
Mail: info@securance.com

Office United Kingdom
Address: 63-66 Hatton Garden
Londen EC1N 8LE, United Kingdom
Tel: +44 (0)20 351 446 56
Mail: info@securance.com

securance.com