NNIT CYBERSECURITY

# A new threat landscape requires a new approach

We make a mark

# Contents

# Protect your business, don’t limit it

## Get an optimized cybersecurity system & setup for your business

In today’s business climate, companies face three security challenges: finding the right level of IT security; managing changing risk scenarios arising from trends such as Internet of Things (IoT), mobility and cloud; and combating increasingly sophisticated cyber threats. In addition, rigorous legislation, such as the EU General Data Protection Regulation (GDPR), is constantly driving the need for dedicated cybersecurity initiatives.

NNIT is a full range cybersecurity provider with a long and proven track record of success. With deep roots in the pharmaceutical industry, we are highly experienced in delivering compliance management, servicing heavily regulated industries, and providing comprehensive business continuity management.

One of our key focus areas is to identify and secure customers’ critical assets and infrastructure. As supply chains and intellectual property become digital, the need to protect critical systems and data is imperative to ensure the reputation and continuity of your business. Our specialized teams leverage their extensive experience and expertise to help your business address its unique cybersecurity risks.

At NNIT, we can help you design, implement and service the right cybersecurity setup, regardless of your industry; a setup that ensures a comprehensive level of IT cybersecurity in every part of your organization, without limiting your business potential. An effective cybersecurity strategy will give you optimal conditions to accelerate business and enable growth. Companies that optimize their cybersecurity are more likely to pursue new technologies, avoid disruption to operations and not least enhance their reputation among their customers. At NNIT we say: **Protect your business, don’t limit it.**

Read on to learn how our cybersecurity services can help your business stay compliant, secure, and future-ready.

# NNIT Cybersecurity Core Principles

CYBERSECURITY CONSULTING

IDENTITY & ACCESS MANAGEMENT

COMPLIANCE & PRIVACY

CLOUD SECURITY

MANAGED DETECTION & RESPONSE

### 1. NNIT IS A FULL-RANGE CYBERSECURITY PROVIDER

We provide end-to-end security services suited to all customers.

### 2. COST EFFECTIVE SECURITY

We take pride in ensuring that we deliver the right level of security, tailored to each customer.

### 3. PROTECTING BUSINESS CRITICAL SYSTEMS

We specialize in protecting our customers' business-critical systems, and safeguarding business operations.

# Cybersecurity Consulting

## Mapping out your route to effective security protection

Businesses are facing serious cybersecurity challenges, and cyber threats are increasing at an alarming rate. These developments require new ways of thinking in order to achieve effective cybersecurity protection and thus avoid financial and reputational damage.

Although you may be aware of the need to step up your cybersecurity, it may not be clear where to start, what activities to launch, or how to prioritize them. Without a clear direction, initiatives can become misplaced, unstructured, and ultimately fail to achieve the desired reduction in your organization's risk profile.

Leveraging our extensive knowledge and expertise from consulting and security activities, we offer a unique range of security advisory services.

We begin with an initial security assessment to help you gain an understanding of your current threat landscape, pain points, and desired risk profile. We then work with you to develop a roadmap for implementation of identified security initiatives – taking into account all aspects of the security landscape; including people, processes and technology areas.

You will benefit from full access to our team of trusted cyber and compliance consultants and technical experts throughout your journey to achieving optimized cybersecurity operations.

# Application Security

## Are your business-critical systems and data secured?

Cybersecurity threats have never been as diverse as they are today, and new threats emerge almost every day. Hackers target the weakest points of organizations in increasingly sophisticated ways, and very often they look to exploit vulnerabilities in applications to gain access to business data or intellectual property.

In the era of digital transformation, the need to secure applications that access business-critical data is higher than ever. It is no longer enough for organizations only to rely on infrastructure security controls to protect their assets. Applications must include built-in security controls to withstand current cybersecurity threats, and organizations must continuously improve the security posture of their applications by adopting secure software-development lifecycle activities such as security training, threat modeling, and security testing.

Considering security throughout the entire software development lifecycle will minimize the risk of security incidents and significantly improve the protection of your business-critical data, while maintaining the agility and productivity of your development teams. Security must be taken seriously, even for non-business-critical applications, in order to prevent attackers from gaining backdoor-access to other critical assets within your organization. In the digital ecosystem, hackers will attack the weakest link.

NNIT's team of application security experts are ready to assist your development teams on their journey to adopt a secure software-development lifecycle. Our services include:

- Secure software-development lifecycle advisory
- Application security health check
- Application penetration testing
- Developer training course in application security principles
- General application security design and implementation advice in areas such as privacy by design, threat modeling, design review, and secure coding.

# Identity & Access Management

## Making it possible for the right people to access the right systems when and where they need to.

As clinical teams seek transformational change, they must operate in a constantly evolving environment. Therefore, transformation projects must consider the ongoing trends that will influence the success or failure of the effort.

Identity & Access Management: Making it possible for the right people to access the right systems when and where they need to. Increasing adoption of technology by businesses and individuals is leading to vastly complex security concerns. Consequently, it is becoming increasingly difficult to maintain control of data and access. As a result, organizations are becoming more vulnerable to security threats, and generally less efficient.

The adoption of cloud-based services presents new challenges and opportunities for managing user identities and access. For this reason, it is vital to have processes and policies to provide the right people with the right access at the right time – in a secure, compliant, and auditable manner.

Identity and Access Management processes grant users controlled access to applications, systems, and files. However, unstructured data falls outside this category and must be addressed specifically. The amount of unstructured data is growing exponentially and it is present in all documents, pictures, emails, and other data repositories. With legislation such as the EU General Data Protection Regulation (GDPR), unstructured data represents a huge risk to organizations.

NNIT can support you on your journey to establishing the policies, processes and the right IAM systems to help you safely administrate and protect your IT infrastructure and sensitive information assets in the future.

**Quality is the core of our business.** Our roots in the pharmaceutical industry ensure that quality, compliance and security are a natural part of our DNA. We understand the importance of delivering the right level of security protection to provide our customers with peace of mind, so they can focus their efforts on core business activities.

– NNIT –

# Compliance & Privacy

## Minimize compliance risk with better control of data flows

Just about all businesses – from the local sports club to major international corporations – process personal data to some extent and are therefore subject to the GDPR. Furthermore, there are also industry-specific requirements that businesses in very tightly regulated sectors have to comply with to protect digital privacy.

In other words, regardless of its size, type or sector, your business probably has a legal and ethical duty to manage data flows properly in order to avoid data privacy breach. The consequences for the company of not doing so can be severe: From a tarnished reputation to fines amounting to millions.

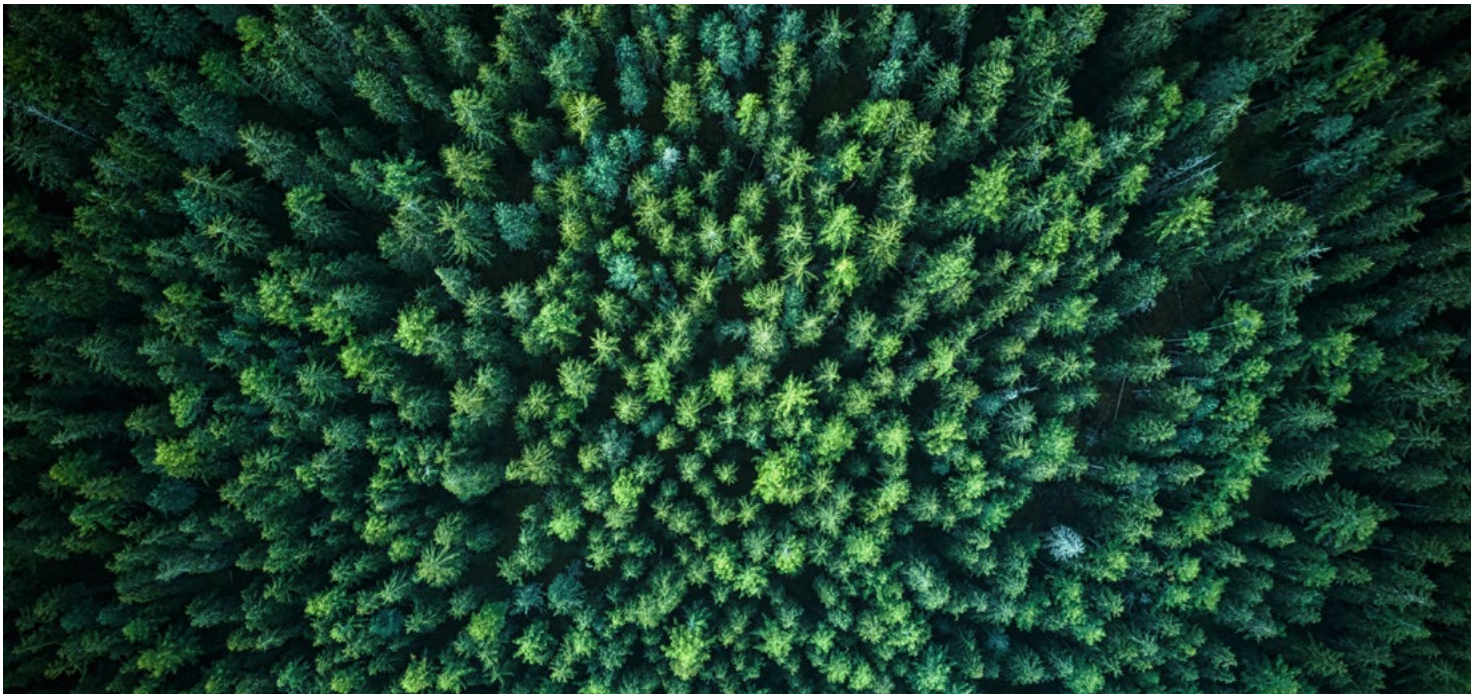
There have been several examples of businesses failing to comply with current regulation. They have failed to manage the processing of personal data and thereby to ensure data-privacy compliance. Heavy fines are often the result of inadequate compliance risk management. Common for all these cases is, that they originate from non-compliance with very basic requirements.

An example could be not ensuring updated data on customers, employees and even suppliers. Another example is managing enormous amounts of data spread over documents on drives, in locally saved folders or in emails.

The key to managing governance risk and compliance framework lies in establishing and maintaining overview, responsibility and processes. This is still a problem for many organizations because of lack of training and knowledge and it results in human error and risky events. Old habits and working methods are hard to change.

Compliance risk management has become an essential discipline for your business to master. With NNIT you get a partner able to manage everything from analysis to advice, and implementation of processes, documentation and delegation of responsibilities concerning compliance-risk concepts.

Our extensive expertise within IT means we can take a holistic approach to compliance & privacy. That means you get a full-stack partner, able to combine advice on compliance-risk management with IT solutions and cyber security.



# Regulatory Compliance

## Staying on top of regulations and industry requirements

In brief, regulatory compliance is about obeying applicable laws, rules and standards with appropriate risk management.

To ensure data privacy compliance, you must fulfill all legal requirements, regardless of the sector or the markets you operate in. This requires knowledge and understanding of which specific policies, rules and documentation apply, and what they mean for your business area. To do this, you need the right procedures, processes and roles in place. You need to ensure these processes are well established within your business, that you comply with them and, in particular, that you can prove that you do so.

At NNIT, we have vast experience of working with compliance consultancy across heavily regulated industries that handle highly sensitive data – from GxP guidelines and regulations to sector-specific standards such as national Executive Orders within data processing.

We use this experience to work with regulations such as the EU General Data Protection Regulation (GDPR), which requires all private businesses and public organizations to implement a sufficient level of IT security and awareness to protect personal data processed in the organization.

NNIT also help clients adhere to the equally important Network and Information Security (NIS and NIS2) Directive and Resilience of Critical Entities (CER) Directive, which requires providers of critical infrastructure services to take appropriate technical and organizational measures to manage threats, networks and information systems.

# Cloud Security & Compliance

## Securing your data in the cloud

Working in the cloud has clearly become the standard approach for the modern enterprise. Nevertheless, there is still considerable confusion regarding how to stay compliant and who is ultimately responsible for the security of cloud infrastructure and applications.

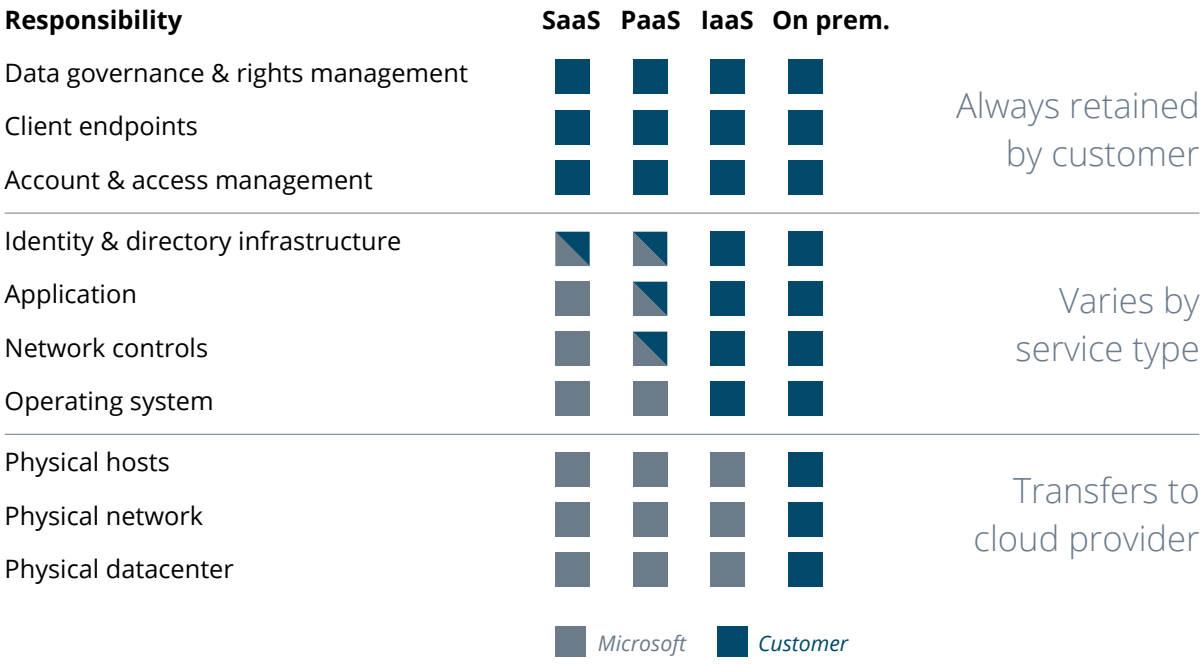
Working in the cloud has clearly become the standard approach for the modern enterprise. Nevertheless, there is still considerable confusion regarding how to stay compliant and who is ultimately responsible for the security of cloud infrastructure and applications.

To help ensure a smooth transition to the cloud, NNIT offers advisory services within compliance and security. In relation to legal obligations, our services include advice on how to comply with regulatory requirements like the GDPR.

When considering and evaluating cloud service providers like AWS and Azure, it is important to understand that cloud security is a shared responsibility and that there are security tasks handled by the cloud provider and tasks that are handled by you.

The workload entailed by these responsibilities varies depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises datacenter.

## Responsibility Zones



**Effective cybersecurity is not about spending more money;** It's about aligning your security initiatives with the threats and priorities for your business in order to protect it from financial and reputational damage.

– NNIT –

# Managed Detection and Response

## Cost-effective management and monitoring of security solutions

Advanced cybersecurity threats and attacks have fundamentally changed the way organizations prioritize and invest in IT security. While preventing attacks is still the primary strategy for securing an organization, breaches will inevitably occur. This makes the need for fast and effective breach detection and response more important than ever.

Managing security systems is a complex and time-consuming task, as it requires the right workforce with the appropriate in-depth technology insight to operate them. This is why organizations are increasingly turning to Managed Security Services as a way to ensure that the organization's fundamental IT infrastructure security is in place, while allowing the organization to focus on its core business instead.

Managed Security Services also allows flexibility, as it allows you to scale your security setup up and down as your need for protection evolves.

With the increasing sophistication of attacks comes increasing detection complexity. Breach detection and response are highly complex tasks, requiring skilled and experienced security professionals who are both hard to come by and expensive to keep on 24/7 rotation.

NNIT offers both traditional operations staffing as well as Detection and Response on security systems with the NNIT Cyber Defense Center. NNIT's value proposition is a systematic approach to managing an organization's security needs. The services cover different functions that include 24/7 monitoring and management of intrusion detection systems, firewalls, log management, patch, upgrades, security audits, security assessments and an incident response service.

Expand your existing protection with true enterprise-class detection and response capabilities with the NNIT Cyber Defense Center. This will provide you with world-class experts on call to assist with security needs 24/7.


NNIT
Cybersecurity
Protect your business,
don’t limit it

# Together we make a mark in business and society; bringing digital transformation to life

**The NNIT Group** provides a wide range of IT and consulting services internationally. In Denmark, where the Group HQ is based, we are one of the leading IT companies, servicing both private and public sector customers across all industries. In the rest of Europe, Asia and USA, we are solely focused on companies within life sciences.

Supporting the entire supply chain, we help optimize internal company processes, production, sales and customer experiences: We advise, build, operate and support, enabling digital transformation and customers to reap the full potential of their organizations. Our role is to foster innovation and make the mark our customers and we aspire to.

The NNIT Group consists of group company NNIT A/S and subsidiaries SCALES, Valiance, Excellis Health Solutions, SL Controls and prime4services. Together, these companies employ over 3,000 people in Europe, Asia and USA.

Read more at **www.nnit.com**

nnit
We make a mark