Governance, Risk & Compliance

The Strong Link Between Business and Cybersecurity

orange™ Cyberdefense

Table of Contents

Cyber Defense – From Risk to Resilience

Digitalization creates enormous opportunities but also opens the door to new risks. As complexity grows and we become increasingly dependent on technology, the attack surface expands, heightening vulnerability to cyberattacks.

It's no longer about avoiding cyberattacks but being prepared when they strike. Because IT forms the backbone of any organization, it's crucial to embed IT security from the start and integrate it as a central part of the business. This overarching responsibility for creating a robust and holistic defense strategy always lies with management.

The Attack Surface Has Never Been Larger

The more digitalized a society is, the greater the attack surface cybercriminals can exploit. Every year, we see more severe cases of DDoS attacks, ransomware extortion, and various types of cyber-activism hitting companies and organizations with significant force. Today, cybercrime has reached a scale that makes it one of the world's largest economies. As cybercriminals constantly improve their use of new technologies, the threat landscape changes. Therefore, we must increasingly prepare for "when" we are attacked - not "if."

Embed Security from the Start

To combat the rise in cyberattacks, we need strong new countermeasures. This requires developing a more holistic approach to cybersecurity. Security must be integrated from the beginning of everything we do to build a sufficiently robust cyber defense.

In the past, cybersecurity was seen as solely an IT department issue - a support function focused on firewalls and perimeter security that the business could technically operate without. For most companies, this has changed drastically. Today, IT plays a vital role in every organization: No IT, no business.

A Robust Defense Requires a Strategy

With IT's growing importance and the evolving threat landscape, it has become the entire organization's responsibility to implement measures and processes to maintain the protection needed to keep core business running - even during large, coordinated cyberattacks. But a robust cyber defense requires more than this. Without a shared framework, an overarching strategy, and competent management, success is unlikely. All of this must be anchored in a responsible leadership team, which, together with employees, is able to enforce and execute the established response plan.

Management Holds the Ultimate Responsibility

The ultimate responsibility for the company's cybersecurity always lies with the board of directors and executive management. The notion of outsourcing this responsibility is outdated. Therefore, from a Governance, Risk & Compliance perspective, it's essential for top management to understand the importance of a strong cyber defense for business survival. This ensures that leaders make informed decisions based on qualified advice from internal or external risk management experts before it's too late and damage is done.

This is where Orange Cyberdefense's Governance, Risk & Compliance expertise comes into play.

In the past, cybersecurity was mainly a task handled by the IT department, but today it is the responsibility of the entire organization.

This places greater demands on communication, and GRC is the language that unites technology, business, and leadership.

Katrine Krogedal | Team Lead GRC
Orange Cyberdefense

Why is Governance, Risk & Compliance Relevant to Cybersecurity?

Together, the three focus areas, Governance, Risk & Compliance, enable you to achieve your cybersecurity goals and build a robust cyber defense in a reliable and efficient way.

Governance focuses on the rules, processes, and structures that guide your organization's decision-making in relation to cybersecurity, ensuring transparency, stakeholder involvement, and alignment with your business goals.

Cybersecurity Risk Management helps identify the risks that could prevent you from reaching your goals. With a well-considered risk profile, you can assess the likelihood and potential consequences of these risks and choose the best cybersecurity strategies.

Compliance ensures that your organization always adheres to all applicable laws and industry standards, avoiding legal issues, fines, and potential damage to your organization's reputation.

Implementing a GRC strategy builds on best practices from standards like COSO, ISO, and NIST. By combining these with well-chosen security solutions and a strong security culture, your organization can be prepared to withstand even major cyberattacks.

orange Cyberdefense

The Strength of GRC

GRC is not just about assessing risks, setting strategies, and making the best decisions. It is also the key to creating a holistic approach to IT security across the entire organization, which is extremely important.

Looking at cybersecurity from a holistic GRC perspective reveals that it's about more than just protecting business-critical data, networks, and systems. It's also about safeguarding people, our relationships, our mutual trust, and the society we are all part of.

A strong GRC strategy within individual organizations and businesses not only significantly improves the ability to withstand cyberattacks and avoid serious business threats but also contributes to making the world we live in a safer and more secure place

Why GRC is a Powerful Management Tool

The strength of GRC lies in more than just assessing risks, setting strategies, and making the best decisions. It also provides a holistic approach to IT security across the entire organization, which is crucial.

Viewing cybersecurity from a holistic GRC perspective reveals that it's about more than just protecting business-critical data, networks, and systems. It's also about safe-guarding people, relationships, mutual trust, and the society we all share.

A strong GRC strategy within each organization creates not only a significant improvement in its ability to resist cyberattacks and avoid severe business threats but also contributes to a safer world.

Where cybersecurity was once a technical task for the IT department, it has now become an essential responsibility for boards and executive teams. With a solid GRC focus, you gain an effective handle on this new management responsibility.

Today, most companies need a security strategy that protects the business without hindering operations, growth, or competitiveness.

This requires the organization to build a shared understanding of the interplay between risk, technology, regulation, and economics - and that is precisely what our GRC advisory services focus on.

Kristine Reme | Security Manager
Orange Cyberdefense

Five Tips for Implementing GRC

The most frequent question our GRC specialists receive is, “How do we get started?” Here are some of their answers:

1 Focus on Compliance
Continuously assess your adherence to relevant laws, regulations, and industry standards. Conduct regular audits and stay updated on legal changes that may affect your organization.

2 Create a Strong Security Culture
Make awareness and accountability for cybersecurity a core value. Reward good security behavior, train employees to recognize and respond to threats, and encourage them to report security incidents without fear of consequences.

3 Define Clear Governance Policies
Establish clear governance policies that specify roles, responsibilities, and decision-making processes for cybersecurity, ensuring alignment with the organization’s strategic goals.

4 Conduct a Risk Assessment
Start by identifying your organization’s unique cybersecurity risks, understanding the threats, and vulnerabilities, and how a security breach could impact you.

5 Implement a Circular Working Model
Cybersecurity should be a top priority in all decisions impacting the organization and core business. Regularly assess the effectiveness of your cybersecurity measures and adjust when needed.

”

The more complex your IT systems become, the more important it is to assess the associated risks.

Here, professional advice and guidance from a strong GRC team can help create close connections between your security and business needs in a way that makes a valuable difference.

Mats Lindblad | GRC Manager
Orange Cyberdefense Sverige

Strategic, Tactical, and Operational GRC

In a world where cyber threats evolve at unprecedented speed, targeted work on Governance, Risk, and Compliance in relation to cybersecurity is necessary for any organization seeking to protect its infrastructure and comply with security regulations. To maximize the benefits of GRC efforts, work should be done holistically on three levels: strategic, tactical, and operational.

The Strategic Level

At the strategic level, GRC is about defining the overall direction and goals for the organization's cybersecurity. Here, governance structures, policies, and frameworks are established to guide how risks are identified, assessed, and managed across the entire company. This level ensures that cybersecurity is integrated into the company's overall strategy and supports its business goals. It provides management with a clear understanding of how cybersecurity initiatives contribute to protecting the company's assets and reputation.

Strategic GRC enables management to make informed decisions based on risk assessments and compliance needs. It builds a strong foundation for resisting cyber threats and ensures that resources are allocated effectively to address the most critical risks.

The Operational Level

The operational level involves daily activities. This includes monitoring security systems, managing security incidents, and maintaining compliance across the organization. Operational GRC ensures that tactical plans are executed effectively and that the organization can respond swiftly to security incidents.

Operational GRC provides real-time protection for the company's assets. It ensures that cybersecurity controls function as they should and that new threats can be addressed quickly. Thus, the operational level is essential for maintaining daily operations without interruptions.

The Tactical Level

At the tactical level, strategic goals are translated into specific action plans and procedures. This level focuses on implementing control measures, risk management, and compliance activities that support the overall strategy. Tactical GRC also involves developing standards and guidelines for all departments and employees within the organization to ensure cybersecurity measures are consistent and effective.

Tactical GRC ensures that strategic decisions can be executed in the operational environment. By implementing tailored controls and procedures that match the company's specific needs, various risks can be minimized.

Why All Levels Are Important

An effective GRC structure requires all three levels to work in harmony. Without a strategic direction, tactical and operational activities may become uncoordinated and ineffective.

Conversely, a strong strategy without effective execution and operational implementation leaves the company vulnerable to threats and compliance breaches. Therefore, it is crucial to invest in all three GRC levels to create a robust defense against cyber threats.

Orange Cyberdefense's Unique Approach

Our GRC advisory services combine technical expertise with a deep understanding of business strategies and compliance needs. We don't just provide strong advice; we help implement and monitor recommended solutions. What sets us apart is our commitment to go beyond reports and recommendations - we guide you all the way to success.

Our approach to GRC includes:

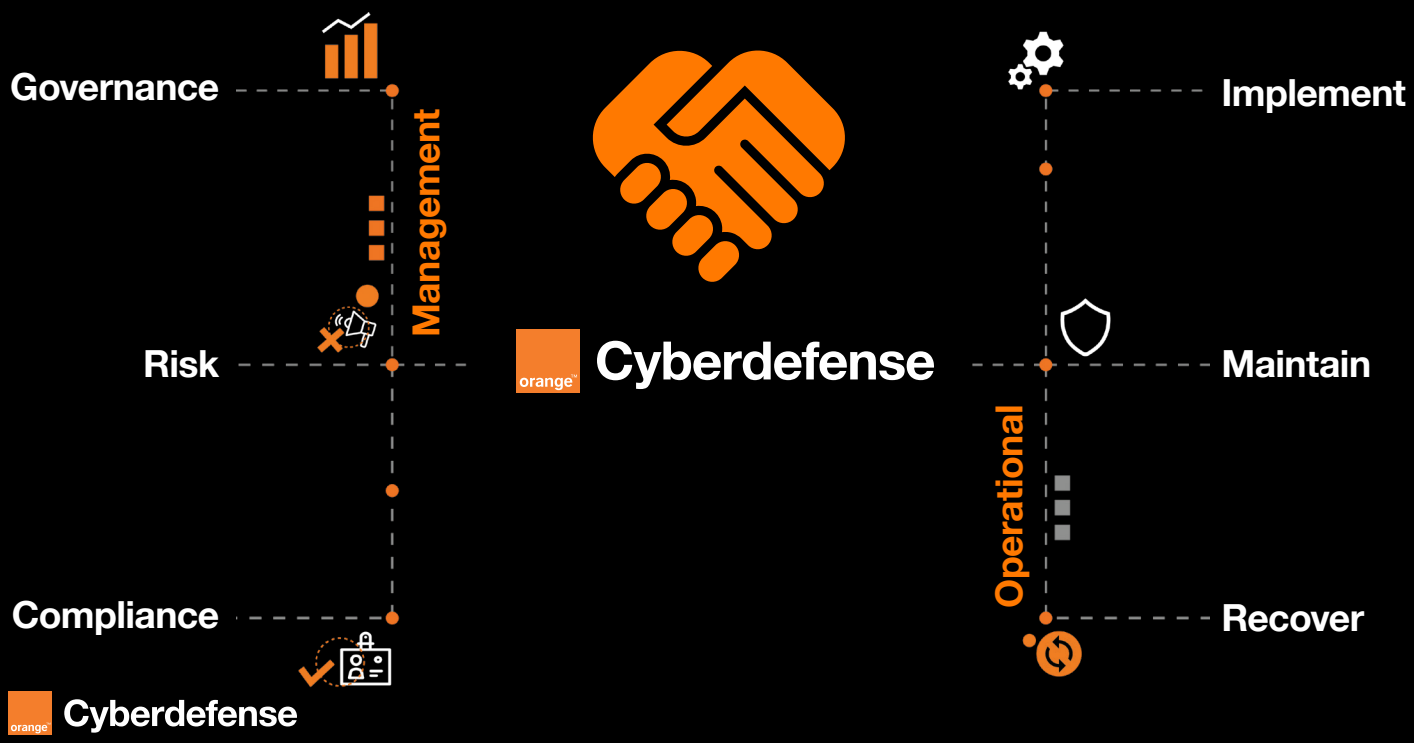
- **In-depth technical expertise:** We understand your complex technological challenges and provide solutions that integrate seamlessly with existing systems.
- **Practical implementation:** We not only help you develop strategies but also offer tactical and operational support to bring them to life.
- **Continuous monitoring and improvement:** We provide not just "one-time solutions" but ensure that your overall cybersecurity strategy is continuously adapted and optimized as the threat landscape evolves.

By choosing Orange Cyberdefense as your GRC partner, you gain not only advice on how to create a strong Governance, Risk, and Compliance strategy and what it means for the robustness of your cyber defense.

We also assist in implementing effective GRC throughout the organization through a practical, hands-on approach that ensures your cybersecurity is always ahead of the latest threats, technologies, and regulations.

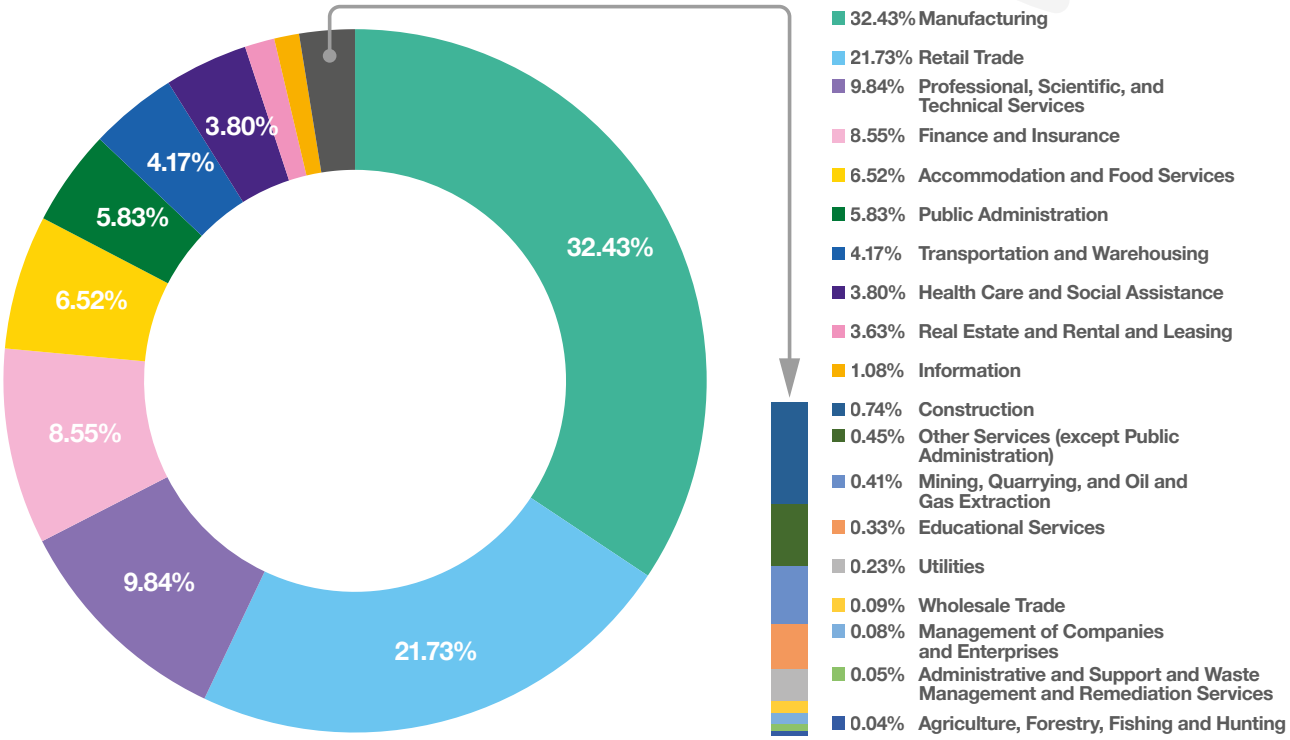
Orange Cyberdefense has an international team of investigators and analytical experts who constantly monitor the global threat landscape and identify current and emerging threats 24/7. Therefore, we can provide you with concrete recommendations on how to best adapt your security strategy so that you are not only protected against existing threats but also prepared for future challenges. Furthermore, we ensure that your systems are always updated with the latest security patches, that your compliance structure meets the latest regulatory requirements, and that your risk management is proactive rather than reactive.

By staying ahead of both technology and threats, you can minimize risks, optimize security resources, and ensure the continuity of your business operations, even in a dynamic and complex cybersecurity environment.

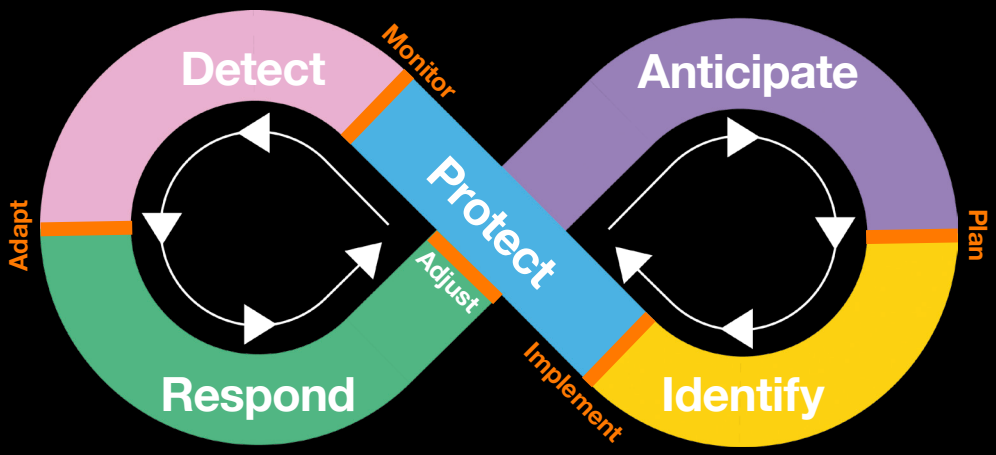


The Current Threat Landscape

Which industries are most often targeted by cyberattacks?



Orange Cyberdefense supports you all the way to the finish line



The current threat landscape is complex, and the number of cyberattacks is increasing. As a recognized security advisor and leading Managed Security Service Provider, Orange Cyberdefense can guide you on how to secure your business, manage vulnerabilities, and build the resilience needed to defend your business against threats.

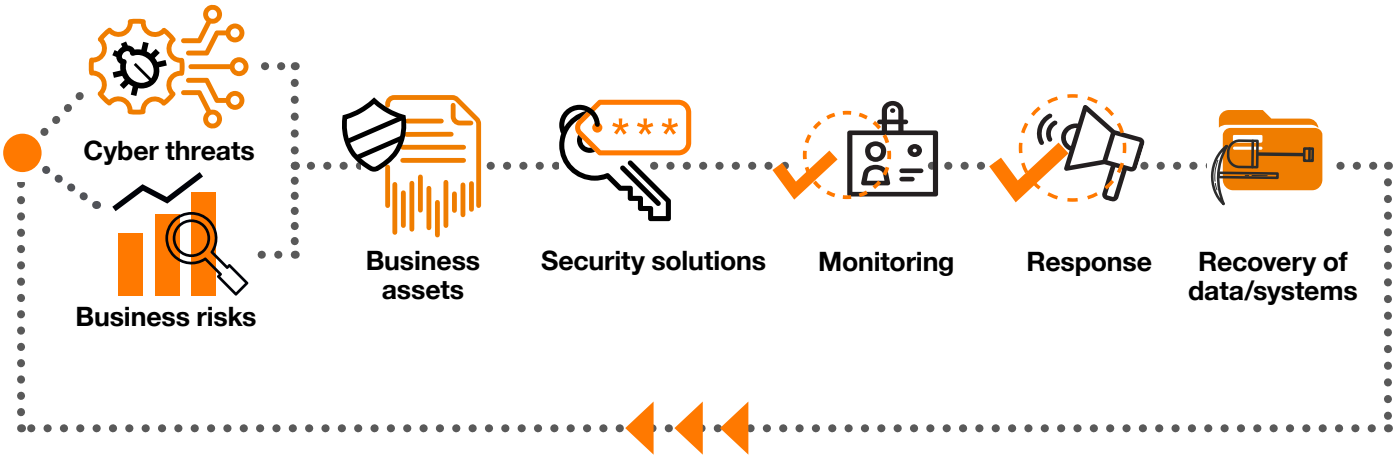
As a GRC partner, we focus not only on strategic management but also consider the operational aspects of GRC just as essential. With deep IT technical knowledge and insight, we are equipped to assist with the implementation and management of your operational security. We provide recommendations and deliver reports that encompass all facets of your cybersecurity. We support you every step of the way, from developing a robust GRC strategy focused on optimizing your cyber defenses to assisting in finding the right security solutions tailored precisely to your needs, risk profile, and resources.

orange Cyberdefense

This is What a Typical GRC Process Looks Like

No organizations are exactly alike, and therefore a GRC process will vary. However, it often consists of different variations of this basic model.

Many executives feel challenged by the increasing need to take direct responsibility for the organization's cybersecurity - this is especially true for management teams and boards in companies dealing with critical societal areas. From a management perspective, the same principle applies to all organizations: The foundation of a strong cyber defense is about creating maximum synergy between the overall business strategic decisions and policies, the daily work processes, and operational security.



Sharp focus on your risks

Early in the GRC process, Orange Cyberdefense's GRC team helps sharpen your focus on your risks and identifies which business data, applications, and infrastructures you should best protect. The goal is to determine what is most critical for your organization so that your business can continue to operate, regardless of what you are exposed to. It is always your risk profile that dictates how your specific cyber defense should be designed and constructed. Over time, the assessment should be repeated and adjusted as new needs arise, as the world does not stand still. Developments always bring about changes, necessitating the ongoing calibration of your cybersecurity solutions and initiatives. It's a circular process.

When we start the analysis work, it often turns out that the most important business systems are quite different from what our client expected. This naturally has significant implications for how the entire architecture of the cyber defense should be structured.

Bo Drejer | GRC Manager
Orange Cyberdefense

GRC Services for All Your Needs

Governance Services

Governance is the strategic compass for your cybersecurity. With these services, you can establish clear goals, policies, and strategies—for example, for the protection of sensitive business data, encryption, and access control that closely reflect your security profile.

Security Strategy

We help assess your organization's risks and security maturity, after which we work closely with your CISO and key business stakeholders to develop an operational security strategy.

CISO-as-a-Service

We provide a flexible, business-driven, and operational CISO-as-a-Service dedicated to advising you on the company's risk profile in relation to the current threat landscape, leading your strategic and tactical cybersecurity projects, managing the daily responsibility for your security governance and information security management system (ISMS), assisting in implementing the operational aspect of your risk management throughout the organization, and managing your cybersecurity training programs.

ISMS Implementation

We assist you in building an Information Security Management System (ISMS), aimed at ensuring a systematic interplay between processes, technology, and employees, so that the management of your information is based on effective risk assessment and recognized standards such as ISO 27001, NIST, and NSM.

Awareness Training

Based on business-driven risk and threat assessments, we help you design and conduct employee training in good security behavior. This can be for all employees as well as selected high-risk groups. If needed, we can also assist with the selection and implementation of the best awareness and training tools.

Risk & Resilience Services

Risk management is your cybersecurity guard, proactively identifying, assessing, and minimizing risks. It is also through these services that you can plan how to best handle security incidents of all sizes.

Risk and Threat Assessment

Together with your management, we conduct a comprehensive risk assessment, identifying your most critical business functions and associated assets. The results are compiled into a decision-making tool that includes process descriptions, risk management, and a risk matrix, providing management with a complete overview of all relevant risks and possible solution models.

Crisis Management

After conducting a risk and threat assessment, we assist you in developing an emergency plan and organizing effective crisis management with clear descriptions of who should participate, what their roles should be, and what tasks they have in a crisis. Selected employees are trained periodically through realistic exercise scenarios.

Business Continuity Management

Through an analysis where we uncover your business needs along with associated risk assessments, we continuously assist you in developing, testing, and updating the emergency plans that ensure the business can continue, even if you are exposed to cyberattacks.

Disaster Recovery Planning & Testing

Here, our specialists develop and test effective recovery plans for your most critical digital assets. All relevant employees are coached in methodology, frameworks, and operational recovery of your business-critical systems.

Security Architecture

Here, we define a risk-driven security architecture that encompasses applications, networks, and infrastructure. It reflects your critical business risks at all levels and is developed in close collaboration with stakeholders from your IT organization, ensuring that practices and maintenance are solidly anchored.

Compliance Services

Compliance is the beacon that safely guides your organization through legislation, regulations, and standards, through regular audits. When new legislation comes into force, compliance requires a review of processes, updating of policies, and execution of audits to ensure that you comply with applicable regulations.

Cyber Maturity Assessment

Using a strong framework for Cyber Maturity Assessment (CMA), we map the maturity of your cybersecurity across all relevant areas and in relation to your business. This also includes document analysis and interviews with key personnel. The results are presented in a clear report, where we also describe recommended, concrete measures that will gradually enhance your cybersecurity with minimal resources.

Regulatory Compliance Assessments

Based on regulatory requirements such as NIS2, DORA, GDPR, or CRA, we assess your compliance. The assessment includes observations and recommended concrete measures to ensure compliance - both now and in the future.

What Our Customers Say About Us

Orange Cyberdefense assists us with risk assessments, management consulting, and operational implementation of enhanced security architecture and protection of our solutions - based on the state's minimum requirements, NIS2, and ISO 27001. With their assistance, we can focus and strengthen our ability to address the increased cyber threat in a resource-efficient manner.

The Climate Data Agency (Klimadatastyrelsen)

The Climate Data Agency works for a climate-resilient, green, and secure Denmark through digital solutions, data-based mapping, and future-proof infrastructure. The Climate Data Agency ensures that the most relevant data is easily accessible and can be combined across sectors - for the benefit of Danish society. The agency is part of the Ministry of Climate, Energy, and Utilities, which is responsible for the work towards a 70% reduction in greenhouse gas emissions in Denmark by 2030.

Klimadatastyrelsen

MILLUM®

Orange Cyberdefense has been a valuable partner that has helped us navigate the increasingly complex security landscape. Through CISO-as-a-Service and other engagements, they have advised top management on security-related business matters. Additionally, they have assisted us in establishing and implementing an ISMS, implementing a risk management process, and developing cybersecurity contingency plans (ISO 22301). Through our partnership, we have strengthened our efforts in information security.

Millum

Millum is the largest procurement platform for the hotel, restaurant, and catering industry in the Nordics. Established in 2002, Millum connects buyers and suppliers through a digital marketplace that facilitates an efficient procurement process for over 90 customers and 2,500 suppliers. By providing solutions that promote transparency, sustainability, and operational efficiency, Millum plays a central role in simplifying the procurement process. With daily users in Norway, Sweden, and Denmark, Millum supports businesses in their pursuit of sustainable practices through innovative technology.

orange Cyberdefense

What Our Customers Say About Us

The work we have conducted together with the GRC team at Orange Cyberdefense on the CMA has been of great value to us at Biometria. This is partly due to the dialogue we have had during the execution, where we internally calibrated based on the various focus areas outlined in the CMA. But we have also gained an up-to-date status and a description of our cybersecurity hygiene from the result that was prepared. We would like to extend a big thank you to the GRC team, who have guided us safely to the finish line!

Biometria

Biometria is a member-owned and central actor in the Swedish forest industry that measures the timber flowing between the forest and industry. It is an impartial organization that ensures that Sweden's forest owners are secure in their timber trade. Biometria's mission is to support and develop timber trade, logistics, and production in the timber market.

BIOMETRIA

Destination Gotland

We gained a clear picture of our strengths and weaknesses in cybersecurity, both at the technical and organizational levels, which helps us prioritize the right initiatives and plan resources. This has provided us with valuable insights and a concrete plan to strengthen our security routines and reduce risks from external threats after we have made the prioritization. The next step is to improve the entire group's security awareness by continuing to educate and discuss cyber hygiene. This requires small steps and disciplined change management, as it now equally concerns cultural changes as much as technical security within the organization.

Destination Gotland

Destination Gotland operates one of Europe's most modern maritime transport systems. The fleet consists of three high-speed vessels, two of which run on liquefied natural gas (LNG) and biogas (LBG). In 2023, Destination Gotland transported around 1.7 million passengers, 540,000 cars, and 760,000 freight units. During the summer season, Destination Gotland has up to 18 departures per day.

> **At Orange Cyberdefense, we do not just leave behind a security report. We analyze your business and develop solutions that closely match your risk profile and resources - and we stand by your side all the way to ensure that you achieve your goals successfully.**
>
> **Bo Drejer**
> **GRC Manager**
> **Orange Cyberdefense Danmark**

Why Choose Orange Cyberdefense as Your GRC Partner?

In a world where IT plays a crucial role in core business, there is a need for strong cybersecurity partners who do not just deliver reports and then withdraw, leaving the full responsibility for implementing the conclusions of those reports to the individual organizations and companies.

Cybersecurity is a complex matter that requires a certain level of technical insight and specific competencies. These are scarce resources that are in high demand. The requirements for cybersecurity are constantly increasing, and in many organizations, the resources cannot keep pace. As a result, more and more companies are finding it very challenging to translate complicated analyses and recommendations into concrete security measures that meet their growing needs for a strong cyber defense.

The best reports are the ones that are acted upon, while expensive reports that simply gather dust have no real value. This is at the core of our approach to GRC consulting.

At Orange Cyberdefense, we stand by our consulting from A to Z, and we are ready to bring it to life. This means we help you all the way from the initial risk and maturity analysis to the effective implementation and operation of the architectures and security systems that best fit your security needs.

Our GRC service is built on professional knowledge and deep technical insight into the market's best and most competitive security products, methods, and services. Our skilled GRC consultants collaborate - both across the Nordics and globally. At the same time, our GRC team has an experience that enables them to understand your business, decode your unique challenges and needs. Therefore, they can help you create the cyber defense that provides you with the absolute best security for your investments.

Choose Orange Cyberdefense because:

- You want a security partner who can align your business and security strategy.
- We can speak the language of both management and the IT department.
- We stand by our consulting - from the first analysis to the implementation and operation of your operational solutions.
- We ensure that your business can continue to operate during any cyber-attack.

Meet Some of Our Experienced GRC Specialists

At Orange Cyberdefense, we work on GRC projects of all sizes across the Nordic countries. Our specialists can provide comprehensive consulting from initial analysis to the operation of implemented security solutions or participate in parts of your GRC process as needed.

Kristine Reme | Security Manager

Orange Cyberdefense Norway

Kristine Reme is an experienced security consultant within the GRC field. She has experience with compliance towards different frameworks and regulations related to information security, as well as in establishing, implementing, and operating information security management systems (ISMS). This includes establishment of governing documents, risk management, vendor management, audits, etc. At Orange Cyberdefense, Kristine has contributed to various GRC projects, and she is dedicated to understanding client needs and ensuring that security strategy align with business objectives.

Bo Drejer | GRC Manager

Orange Cyberdefense Denmark

Bo Drejer has over 20 years of experience with operational GRC in organizations of all sizes. He is accustomed to communicating and facilitating collaborative processes at both management and technical levels. Bo's experiences span several sectors, including transportation, telecommunications, public service, retail, and finance. He has worked as an independent consultant and has been employed by companies such as PwC, Microsoft, Oracle, IBM, and now at Orange Cyberdefense.

Katrine Krogedal | Team Lead GRC

Orange Cyberdefense Norway

Katrine Krogedal is a senior security advisor in GRC. She has several years of experience in establishing management systems for information security (ISMS), including the development of frameworks, structures, risk management, supplier management, and effective handling of security incidents. She has also assisted several companies in achieving ISO 27001 certifications. In addition, Katrine has extensive experience in developing strategic action plans for enhanced cybersecurity.

Mats Lindblad | GRC Manager

Orange Cyberdefense SWeden

Mats Lindblad has over 25 years of experience working with security in various forms. He has worked in leadership and management at strategic, tactical, and operational levels in both the public sector and private companies, including roles as CISO and CSO. He has also served as a strategic management consultant in various sectors such as banking, insurance, retail, and government authorities. He specializes in resilience issues and helps clients build and maintain their ability to manage the various types of incidents that may arise.

Cyberdefense - Who Are We?

Global positioning

Orange Cyberdefense is a leading European cybersecurity and Managed Security Service Provider with over 25 years of experience. We specialize in delivering consulting, solutions, and services to our customers worldwide. We are recognized as a leading MSS provider by information technology research and advisory companies such as Gartner, Forrester, and IDC.

We have a global Threat Intelligence department, and 250+ analysts spread across **17 SOCs, 15 CyberSOCs, 11 CERTs,** and **4 scrubbing centres** to mitigate DDoS attacks which collect and analyze global data from over **500 information sources 24/7.**

Local presence

In the Nordics, our team consists of **500 employees** across Denmark, Norway, and Sweden. Our Nordic offices are located in Copenhagen & Aarhus (Denmark), Stockholm, Malmo, Gothenburg & Sundsvall (Sweden), and Oslo (Norway).

Our customers include multinational companies, public organizations, and government authorities.

Our growth journey

We have over **3,100 employees** globally and 50,000 customers worldwide of which 6,000 are large enterprises. We have experienced stable economic growth and progress over the years. In 2024, our global revenue was **€1.2 billion.**

Part of Orange Group

Orange Cyberdefense is part of the global French telecommunications group **Orange,** which has 137,000 employees and **296 million customers** worldwide. In 2024, **Orange Group** had a global revenue of **€40,3 billion.**

For more information, visit:
orangecyberdefense.com/dk

Contact us

info@dk.orangecyberdefense.com

+45 70 20 03 32