MONOCEROS
SECURITY

Cyber security Assessment & Gap Analysis
Creating a Clear Overview and Addressing Gaps for Strategic Security Improvement

Identify Gaps & Strengthen Defense

In today's complex Cyber security landscape, organizations face ever-evolving threats. Our Cyber security Assessment & Gap Analysis service provides organizations with a thorough evaluation of their current security measures, identifying critical gaps and ensuring alignment with industry-leading frameworks such as NIST, CIS, and ISO 2700x.

What We Offer

Our service includes a detailed analysis of your Cyber security posture, offering actionable insights and recommendations to fortify your organization's defenses. The primary focus areas include:

- **Framework Alignment**: Reviewing your security controls to ensure adherence to NIST, CIS, and ISO 2700x standards.

- **Gap Identification**: Pinpointing vulnerabilities, compliance deficiencies, and areas requiring immediate attention.

- **Risk Prioritization**: Evaluating and ranking risks based on their potential impact on your organization.

Actionable Recommendations

- **Risk Remediation Plan:** Detailed recommendations for closing identified gaps.

- **Security Roadmap:** Steps to achieve full alignment with NIST, CIS, or ISO 2700x requirements.

- **Comparative results through known frameworks:** A maturity evaluation through worldwide known frameworks such as NIST, CIS or ISO 2700x.

Comprehensive Assessment

We take a structured approach to evaluate your organization's Cyber security capabilities:

- **Policy and Procedure Review**

  - Assessing governance structures and operational policies.

  - Validating the adequacy of existing procedures against best practices or relevant regulations such as NIS2/DORA/CER or similar.

- **Infrastructure & Data Security Analysis**

  - Evaluating data protection mechanisms, including encryption, access controls, and backup strategies.

- **Incident Response Readiness**

  - Reviewing the organization's preparedness to detect, respond to, and recover from security incidents.

  - Assessing historical breach data to uncover systemic weaknesses.

Cyber security Assessment & Gap Analysis
Creating a Clear Overview and Addressing Gaps for Strategic Security Improvement

MONOCEROS SECURITY

How We Work

Our advisors collaborate closely with your organization to ensure the results are both practical and strategic:

- **Initial Assessment**: A high-level review of your existing security framework and processes.

- **Detailed Gap Analysis**: Deep-dives into specific domains such as governance, risk management, IT infrastructure, and compliance.

- **Deliverables**: Clear, actionable findings and recommendations in an easy-to-understand report format.

What you get:

With a Cyber security Assessment & Gap Analysis, you will gain a clear understanding of your organization's current security posture, including strengths, vulnerabilities, and areas for improvement:

- A thorough understanding of the target organization's Cyber security risks and strengths.

- Compliance Confidence: Alignment with globally recognized frameworks like NIST, CIS, and ISO 2700x to fit relevant legislation.

- A prioritized action plan for mitigating found vulnerabilities.

- Expert guidance for integrating Cyber security post-acquisition.

- Recommendations for use in the negotiation process for the acquiring company.

The Results

With our Cyber security Assessment & Gap Analysis, you will:

- Reduce risk exposure through initiative-taking measures.

- Gain overview and prioritize actions to build a resilient and compliant Cyber security posture.

- Gain confidence in your organization's ability to withstand cyber threats.

At Monoceros Security, we are committed to helping your organization anticipate, manage, and mitigate risks with clarity and confidence. Together, we will create a secure and resilient environment that empowers you to achieve sustainable success in an uncertain world.

PER SILBERG HANSEN
Executive Advisory – Risk and Cyber security

MONOCEROS
SECURITY

BACKGROUND

A seasoned professional with extensive experience across Cyber Security and Risk Management, including IT Security Leadership, Crisis Management, Supply Chain, and Value Chain Risk Management at operational and strategic levels. Proven ability to excel in cross-functional collaboration across global organizations, engaging effectively with teams and stakeholders at all levels.

KEY COMPETENCIES

Expert in driving pragmatic, business-focused solutions that deliver measurable value outcomes, including Risk Management, IT Disaster Recovery, Crisis Management, and Cyber Security Strategies.

Skilled in balancing business operations with project objectives, ensuring alignment with strategic goals and communicating effectively with project owners and key stakeholders.

Excels in creating impactful results through Leadership, Mentorship, Development, and Empowerment, with a preference for tasks involving broad responsibilities and high business impact.

PROFESSIONAL EXPERIENCE

Former roles include senior leadership positions at Prueba Cyber security, Improsec – Itm8, Sydbank A/S, Bestseller A/S, Ecco Sko A/S, and Danfoss A/S.
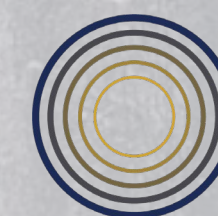
Demonstrated success in implementing high-value projects and fostering organizational resilience

EXECUTIVE ADVISORY
- Working with boards and executive management
- Business Continuity / Crisis Management
- Enterprise Risk Management
- Cyber Risk Management
- Building security strategies and roadmaps
- Security investments and organizational development
- Advising existing Security Management or acting as interim CISO

CERTIFICATIONS
- Bestyrelsesuddannelse – Executive Cognito
- CISM (Certified Information Security Manager)
- CISSP (Certified Information Systems Security Professional)
- ESL (Eksamineret Sikkerhedsleder)
- ITIL Foundation V3

PER SILBERG HANSEN

Executive Advisory – Risk and Cyber security

+45 5130 3200
psh@monoceros.dk
linkedin.com/in/silberg/

Experience with large events

- Crisis Management at +20 cyber attacks
- Communication crisis / "Shitstorms"
- Server breakdowns, network failure, etc.
- Natural disasters (major flooding, mud volcano)
- Fire, toxic gas outlet
- Strike
- Riots
- Several large fraud investigations