FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON **DBD.AU.DK**

BUILDING BLOCKS

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Alignment between business and security

Task

Business strategic task:

That the company achieves/has:

A clear understanding of the business and operational objectives of IoT solutions that is in line with an awareness of the criticality of cybersecurity for both business and operations.

Supporting questions for idea catalogue

1. Does the company understand the business objective of its IoT solutions? For instance, optimisation, attracting new customers, enabling better decision-making, or extending the service life of production equipment?
2. Does the company understand how critical cybersecurity is for business (also called criticality)?
   a. **Confidentiality**: What would the consequences be for your business if data from your IoT sol utions were made public? For instance, production data.
   b. **Availability**: What would the consequences be for your business if your production data and systems were unavailable?
   c. **Integrity**: What would the consequences be for your business if unauthorised persons could alter your data and – potentially – make it incorrect? For instance, settings on production machinery, or drawings.
3. Can cybersecurity form the basis for new business opportunities and business cases? For instance, ensuring that production is not delayed.

Idea catalogue for further development

Write down ideas for next step(s) in the business strategic task related to IoT cybersecurity.

1. Criticality of cybersecurity in the company, depending on the purpose of the IoT solutions.
2. Potential for new business opportunities, resulting from developing the company's cybersecurity.
3. Coordination of cybersecurity tasks with other development initiatives in the company, such as strategy initiatives, quality management, procurement of new machinery or new technology, or starting up production of new products or services.

INDUSTRIENS FOND

"CyPro", supported by Industriens Fond.

UGLAINSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS

BUILDING BLOCKS

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Approach to security and risk

Task

Task relating to risk mindset and specific initiatives for IoT cybersecurity:

That the company achieves/has:

A risk-based and dedicated approach to the cybersecurity of IoT solutions.

Supporting questions for idea catalogue

1. Has the company actively considered how to deal with potential threats and risks of attacks on IoT systems and data?
2. Has the company implemented procedures for risk assessment and threat modelling for IoT solutions?
3. Do managers and employees share the same risk-based mindset regarding potential attacks on IoT systems and data?

The company's idea catalogue for continued development

Write down ideas for next step(s) in the company's approach to IoT cybersecurity and risk:

1. Company's approach to risk regarding IoT solutions.

2. Shared knowledge and common mindset concerning the approach to risk and IoT cybersecurity in the company.

"CyPro", supported by Industriens Fond.

FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON DBD.AU.DK

BUILDING BLOCKS

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Regulation and standards

Task

Task concerning regulation and standards:

That the company achieves/has:

The capability to apply relevant standards for IoT cybersecurity to ensure compliance with existing regulation, or

The capability to identify and prepare for forth-comming regulation and standards in this field.

Supporting questions for idea catalogue

1. Has the company actively considered how to implement regulation (existing and forthcoming) and standards relevant for IoT cybersecurity?
2. Is IoT cybersecurity an integral part of the company's ongoing quality management?
3. Has the company allocated specific resources to work with guidelines and standards for IoT cybersecurity?

The company's idea catalogue for continued development

Write down ideas for next step(s) in the company's work with regulation and standards for IoT cybersecurity.

1. The company's opportunities / challenges in relation to working with standards for IoT cybersecurity.

2. Relevant IoT cybersecurity regulation.

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS

FIND OUR WEBISTE
DIGITAL BUSINESS DEVELOPMENT
ON DBD.AU.DK

BUILDING BLOCKS

Scan the QR code to find a step-by-step guide for this tool, digital business development cases and further inspiration at dbd.au.dk

Building block: Processes and organisational integration

Task

Organisational integration task:

That the company has decided to:

Assign the responsibility for IoT cybersecurity to one or more individuals in-house or externally, who continuously focus on the development of the company's cybersecurity for IoT.

Supporting questions for idea catalogue

1. Has the company identified the need for collaborating with external partners /consultants on IoT cybersecurity?
2. Is the responsibility for IoT cyber-security in the company assigned to one or more specific individuals (in-house or externally)?
3. Has the company developed a structured plan incl. objectives and specific initiatives for IoT cybersecurity in the company?
4. Has the company allocated time and resources for building up in-house IoT cybersecurity competence?

The company's idea catalogue for continued development

Write down ideas for next step(s) in the company's work with processes and organisational integration of IoT cybersecurity

1. Responsibility for IoT cybersecurity.
2. Employee involvement in IoT cybersecurity.
3. Plan and competence development in IoT cybersecurity.

"CyPro", supported by Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY
AARHUS BSS