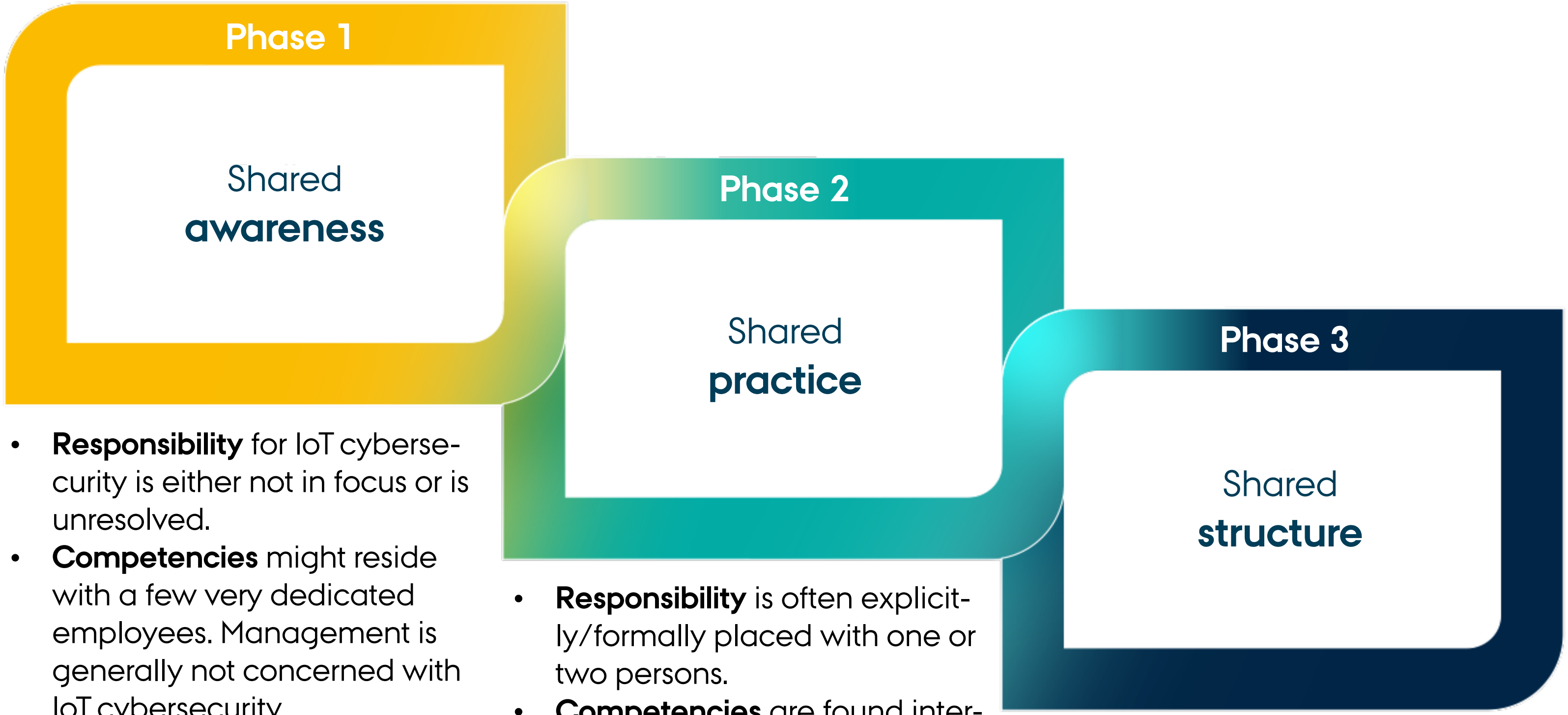
KEYWORDS SHEET: ORGANISATION

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



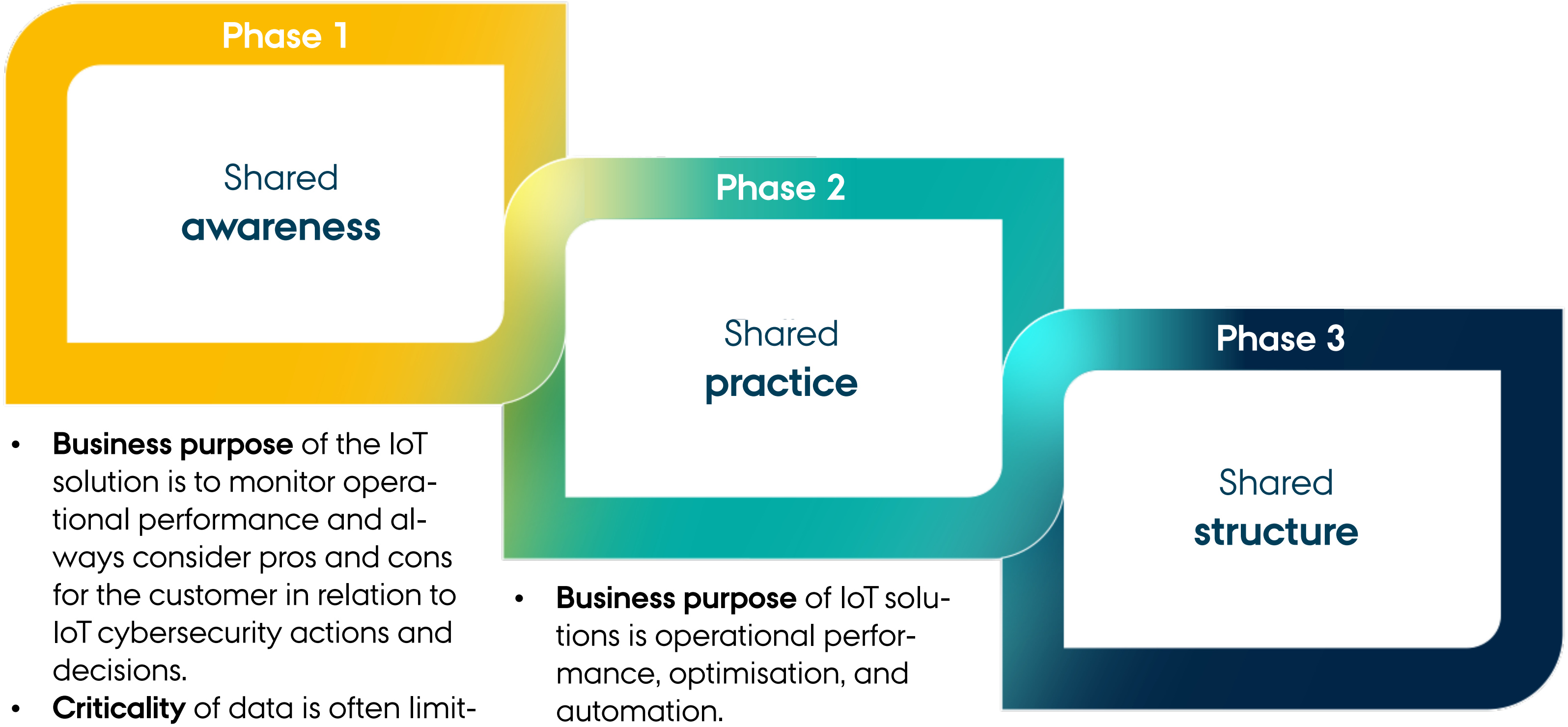
- **Responsibility** for IoT cybersecurity is either not in focus or is unresolved.
- **Competencies** might reside with a few very dedicated employees. Management is generally not concerned with IoT cybersecurity.
- **Approach** is often a response to customer inquiries. No contingency plans or other organising initiatives.

- **Responsibility** is often explicitly/formally placed with one or two persons.
- **Competencies** are found internally with some persons. Often sparring with external consultants. Management is generally concerned with the financial consequences associated with IoT cybersecurity.
- **Approach** is centred on creating a shared understanding and building plans and procedures.

- **Responsibility** is clearly defined, organised and anchored.
- All needed **competencies** are available internally or externally. Management is an active and informed decision partner regarding IoT cybersecurity.
- There is a structured **approach** to incidents and risk management for all parts of the business.

KEYWORDS SHEET: BUSINESS

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



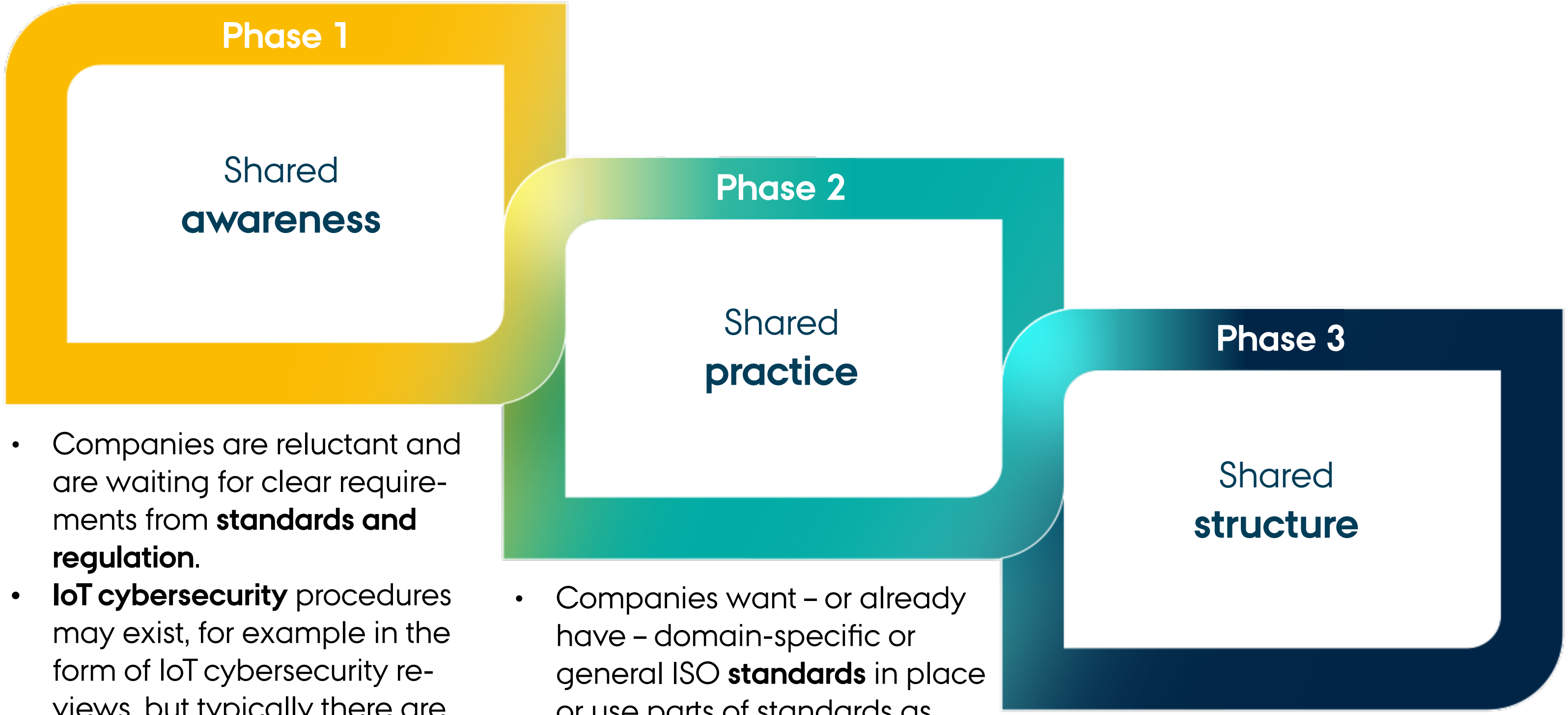
- **Business purpose** of the IoT solution is to monitor operational performance and always consider pros and cons for the customer in relation to IoT cybersecurity actions and decisions.
- **Criticality** of data is often limited to confidentiality.
- **Business development** is not related to or relevant for IoT solutions.

- **Business purpose** of IoT solutions is operational performance, optimisation, and automation.
- **Criticality** of data is often related to integrity and availability. Business is focused on the cost-effectiveness of IoT cybersecurity.
- **Business development** is often viewed as securing data to ensure confidentiality and integrity in potential new cloud services offered to customers.

- **Business purpose** is automation and connected services and products.
- **Criticality** of data and risk appetite is customised for each IoT solution.
- **Business development** involves new business models where IoT cybersecurity is seen as a 'selling point'. Cloud services and digital platforms are offered to customers.

KEYWORDS SHEET: QUALITY

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



Phase 1

Shared **awareness**

- Companies are reluctant and are waiting for clear requirements from **standards and regulation**.
- **IoT cybersecurity** procedures may exist, for example in the form of IoT cybersecurity reviews, but typically there are only few routines and many ad hoc solutions.
- **Use of standards** is viewed as a possibility, but the certification process is considered overwhelming.

Phase 2

Shared **practice**

- Companies want – or already have – domain-specific or general ISO **standards** in place or use parts of standards as guidelines.
- **IoT cybersecurity** procedures are informed by general levels and goals. Increasing focus on the entire IoT solution landscape.
- **Use of standards** is regarded as a method to establish a shared language both internally and externally and as a valid foundation for decision-making.

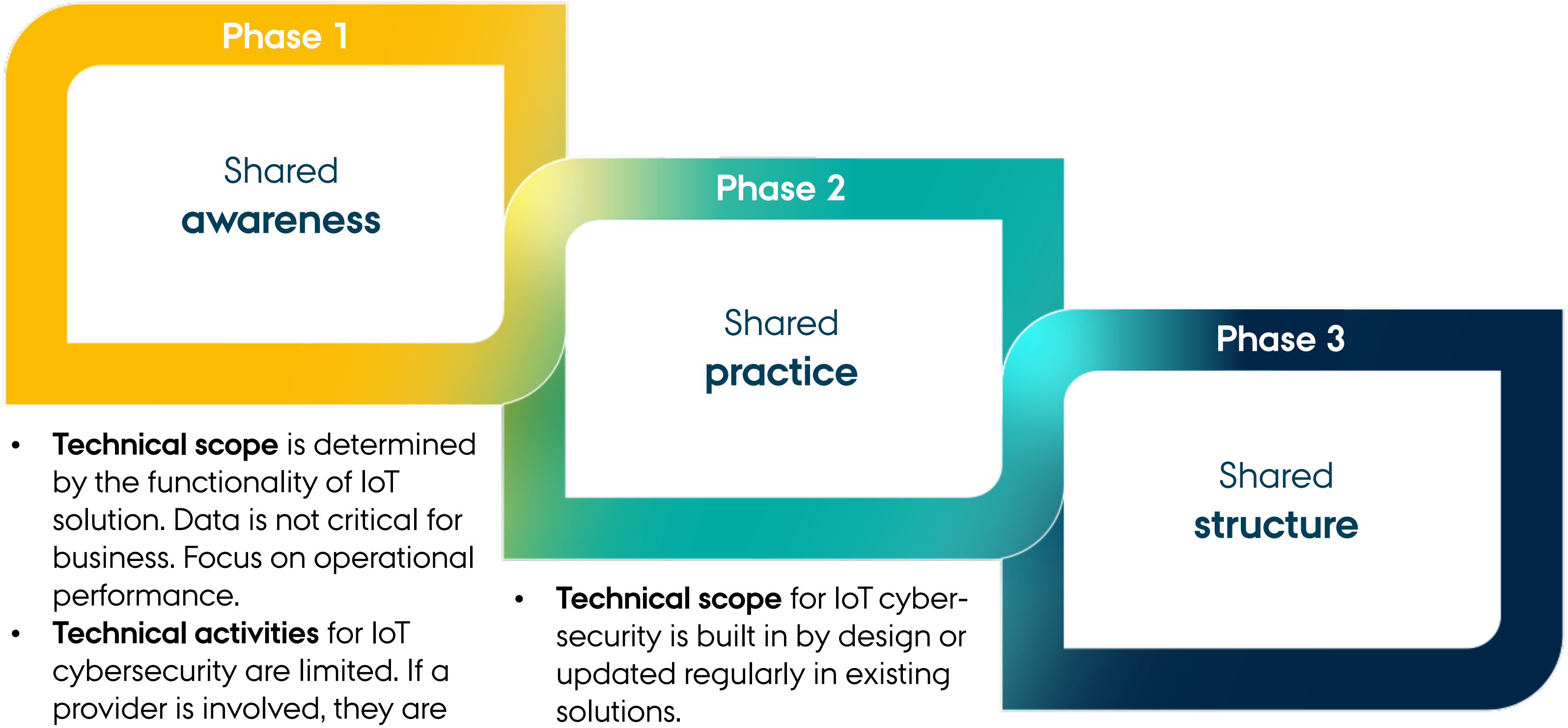
Phase 3

Shared **structure**

- Companies often have relevant domain-specific ISO, IT and cybersecurity **standards**, which makes it easier to comply with regulation.
- **IoT cybersecurity** procedures are anchored in frameworks and in security by design procedures.
- **Use of standards** provides a shared language and is considered a competitive advantage for the business.

KEYWORDS SHEET: TECHNICAL

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



Phase 1

Shared **awareness**

Phase 2

Shared **practice**

Phase 3

Shared **structure**

- **Technical scope** is determined by the functionality of IoT solution. Data is not critical for business. Focus on operational performance.
- **Technical activities** for IoT cybersecurity are limited. If a provider is involved, they are expected to manage IoT cybersecurity. Some patching occurs, but few companies maintain logs, and there is little focus on user access to various devices.
- **Risk management** is not explicit or systematic.

- **Technical scope** for IoT cybersecurity is built in by design or updated regularly in existing solutions.
- Necessary IoT cybersecurity competencies to carry out **technical activities** are available. Patch management, logging, monitoring and user access are systematised.
- **Risk management** is seen as a shift from performing ad hoc tasks to establishing a risk-based approach to IoT cybersecurity.

- **Technical scope** is based on a holistic approach where all use scenarios and all IoT solutions are assessed.
- **Technical activities** are conducted in shared and structured processes. Several layers of IoT cybersecurity are often present, and dedicated resources have been allocated.
- **Risk management** is an ongoing process that both managers and employees contribute to.