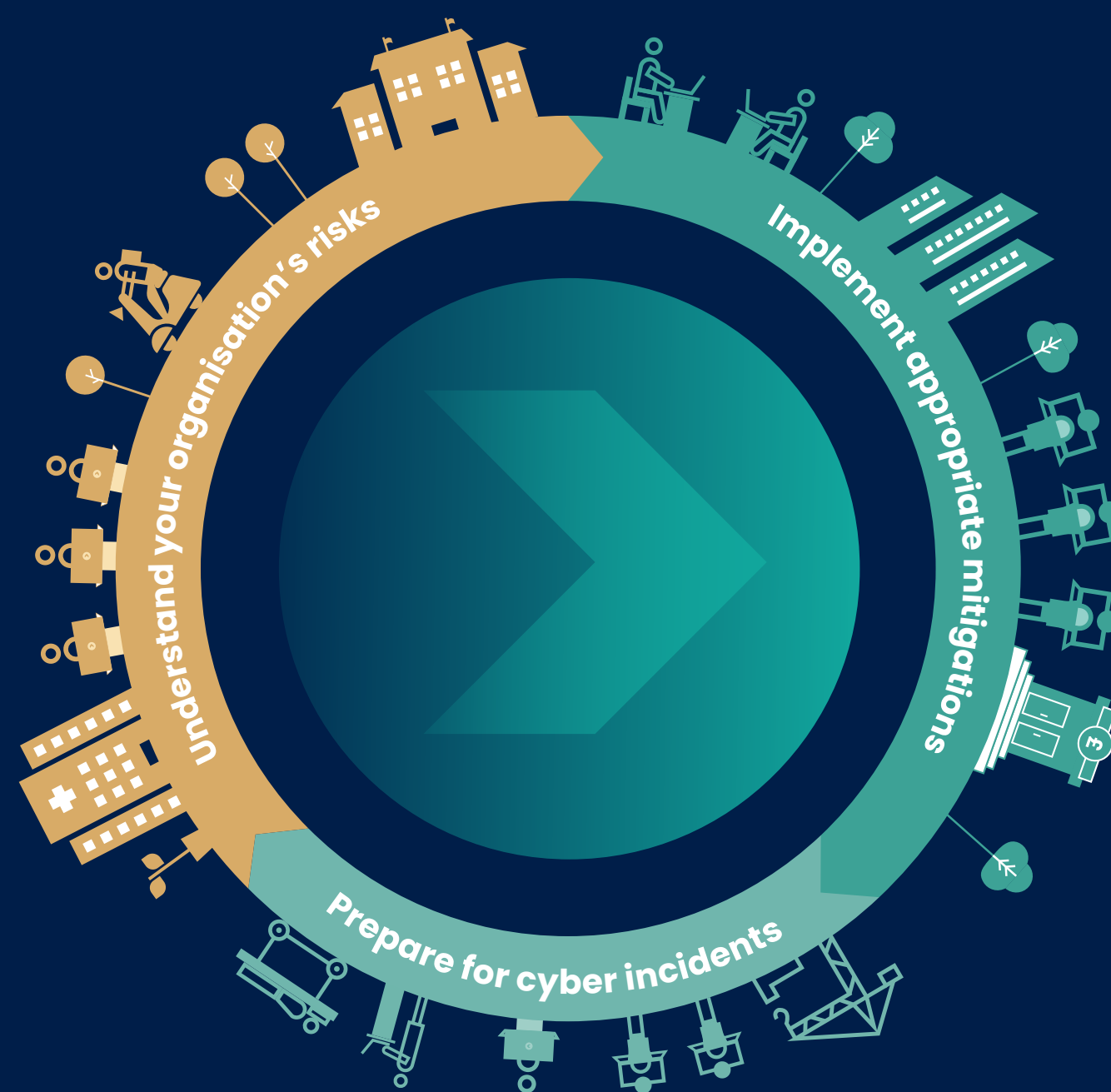




National Cyber  
Security Centre  
a part of GCHQ

# 10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.



## ➤ Risk management

Take a risk-based approach to securing your data and systems.

## ➤ Engagement and training

Collaboratively build security that works for people in your organisation.

## ➤ Asset management

Know what data and systems you have and what business need they support.

## ➤ Architecture and configuration

Design, build, maintain and manage systems securely.

## ➤ Vulnerability management

Keep your systems protected throughout their lifecycle.

## ➤ Identity and access management

Control who and what can access your systems and data.

## ➤ Data security

Protect data where it is vulnerable.

## ➤ Logging and monitoring

Design your systems to be able to detect and investigate incidents.

## ➤ Incident management

Plan your response to cyber incidents in advance.

## ➤ Supply chain security

Collaborate with your suppliers and partners.