CYBER
SECURITY
AWARENESS
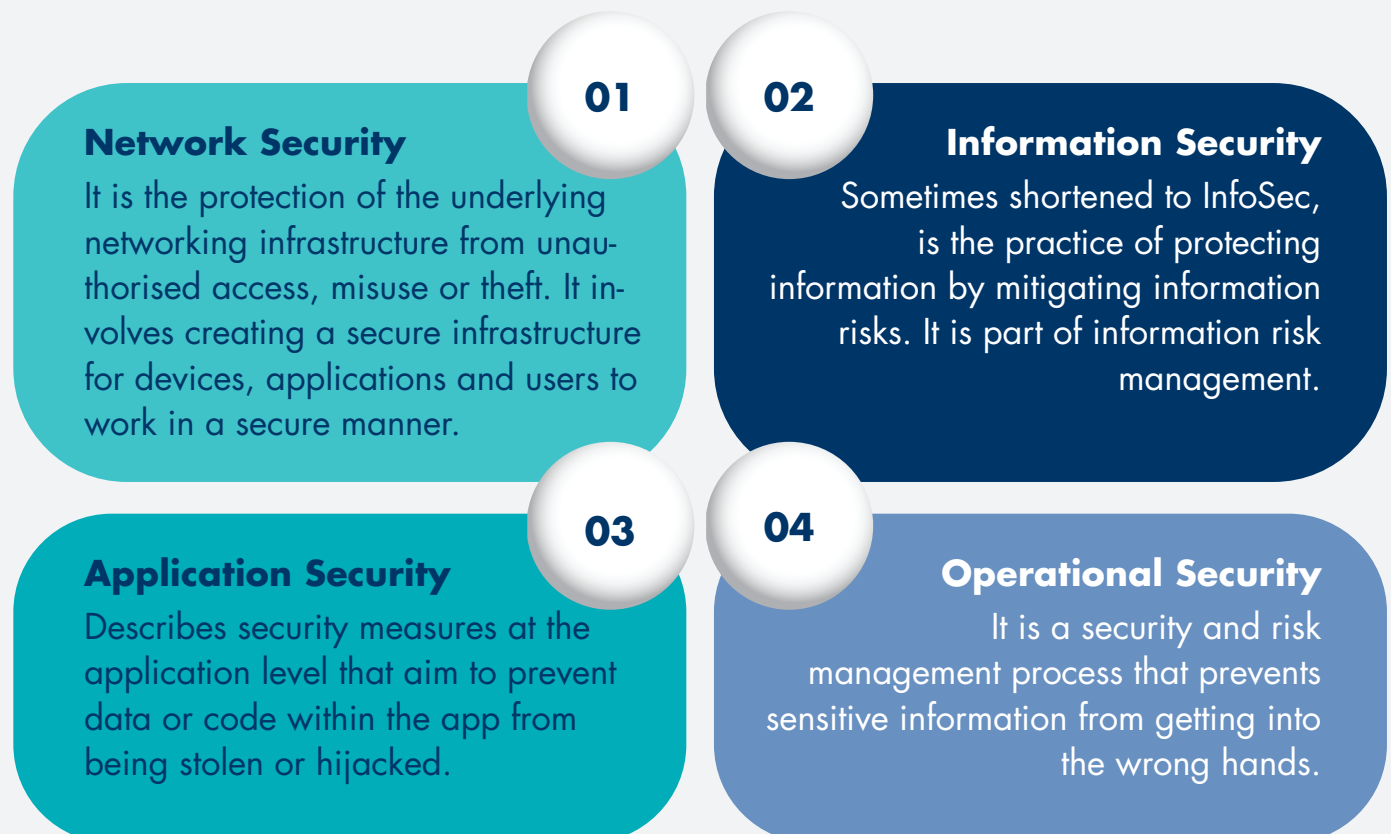
CSIR

Touching lives through innovation

Cybersecurity Controls

Cybersecurity is a multidimensional risk management process comprising diverse security controls to maintain the confidentiality, integrity and availability of information and communication technologies.

Security Control Measures
- Technology
- Policy and Practices
- Human Factors

ICT & People

Ideal Characteristics
- Confidentiality
- Integrity
- Availability
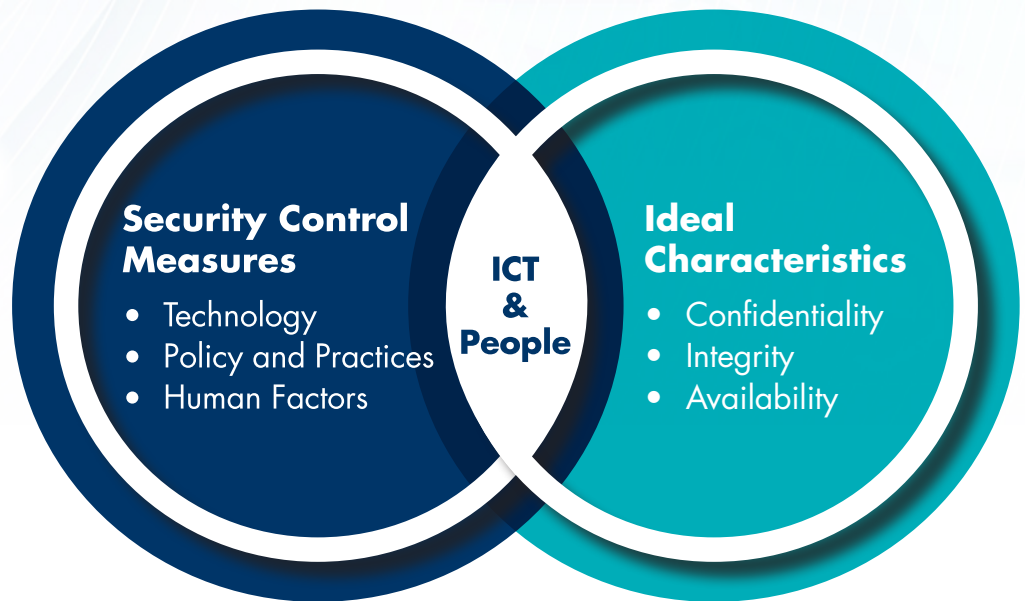
Technology Security Controls

Technology control measures are put together to protect an organisation's critical information infrastructure, which includes the network infrastructure, software programs and applications, hardware or operational equipment, data and information, and individuals.

01

Network Security
It is the protection of the underlying networking infrastructure from unauthorised access, misuse or theft. It involves creating a secure infrastructure for devices, applications and users to work in a secure manner.

02

Information Security
Sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information risk management.

03

Application Security
Describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

04

Operational Security
It is a security and risk management process that prevents sensitive information from getting into the wrong hands.

# CYBERSECURITY AWARENESS

ICSC's Technology Controls

Tools that were developed inhouse by the CSIR's Information and Cybersecurity Centre (ICSC).

1. Educyber

Educyber is an open-source, web-based eLearning platform. It was implemented to educate students/employees about cybersecurity awareness and best practices when using the Internet. The purpose of this platform to sharpen the understanding of cyber threats and vulnerabilities. You can use it to access available online awareness training to enhance your learning experience through videos, quizzes, posters, podcasts, etc.

Below is a summary of the courses and content that employees can use to learn:

• Introduction to cybersecurity awareness
• Legal and ethics of cybersecurity and password protection
• Social media awareness
• Email and mobile security
• Web and cloud security
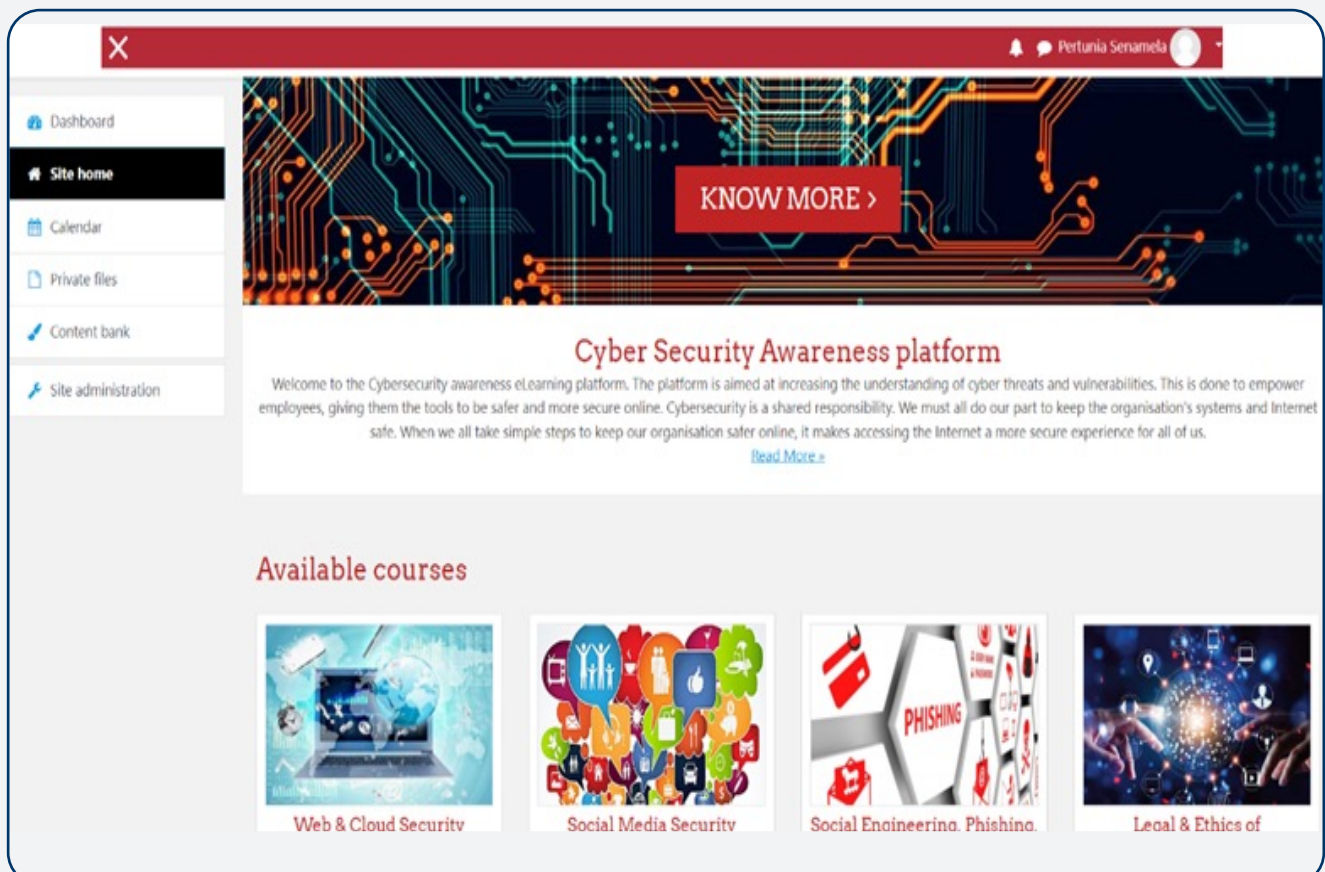
2. Network Emulation and Simulation Laboratory (NESL)

NESL provides a web-based environment for cybersecurity researchers with the ability to perform network bandwidth modelling, cybersecurity training, device research and advanced analytics to study cyber risks and deliver effective and practical security solutions. This is a system designed to bring together researchers and experts from various universities across South Africa to drive developments in the theory and practice of cybersecurity to ultimately deliver innovative security technologies.

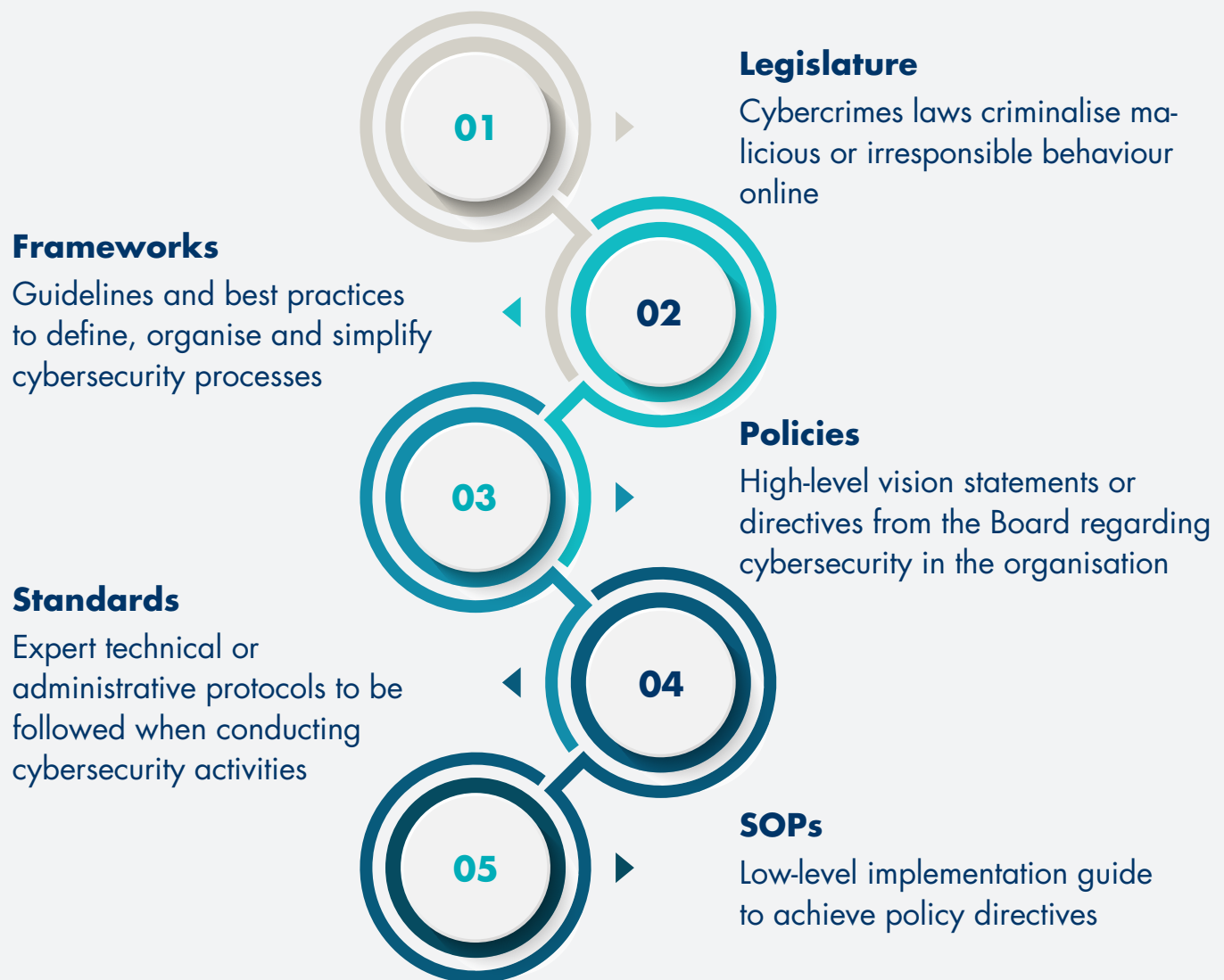## The main goals of the NESL platform include:

- Enhancing cybersecurity skills development in South Africa
- Provisioning coordination, as well as research and development leadership across national and municipal government, the private sector and academia improve cybersecurity research

Policy and Practices Security Controls

Cybersecurity policy and practices are regulatory and legislative control measures, including cybersecurity laws, frameworks (i.e., best practices and guidelines), policies, standards and standard operating procedures (SOPs), that direct and control (i.e., govern) the implementation of cybersecurity processes within an organisation, thus facilitating compliance and a cybersecurity culture.

01

Legislature

Cybercrimes laws criminalise malicious or irresponsible behaviour online

Frameworks

Guidelines and best practices to define, organise and simplify cybersecurity processes

02

03

Policies

High-level vision statements or directives from the Board regarding cybersecurity in the organisation

Standards

Expert technical or administrative protocols to be followed when conducting cybersecurity activities

04

05

SOPs

Low-level implementation guide to achieve policy directives

"I really think that if we change our own approach and thinking about what we have available to us, that is what will unlock our ability to truly excel in security. It's a perspectives exercise. What would it look like if abundance were the reality and not resource constraint?"

- Greg York (Director, Cyber Security & IT Privacy at Follett)

Human Factors Security Control

The human factors security control is a combination of cybersecurity awareness, education and training programmes that equip individuals with cybersecurity skills.

Below are the tips you need to teach yourself about Internet and social media safety:

First, do not harm! Do not use the Internet or social media to attack or harm anyone or their reputation.

Things you post may be **VERY** difficult to erase – so think carefully about your future before posting!

Just because you see it online, does **NOT** mean it is true! Fact-check before sharing fake news.

Recognise when a post is calculated to trigger you emotionally and engage the rational part of your brain before reacting or sharing.

Websites and social media platforms collect **A LOT** of information about you and **WILL** use it to manipulate you!
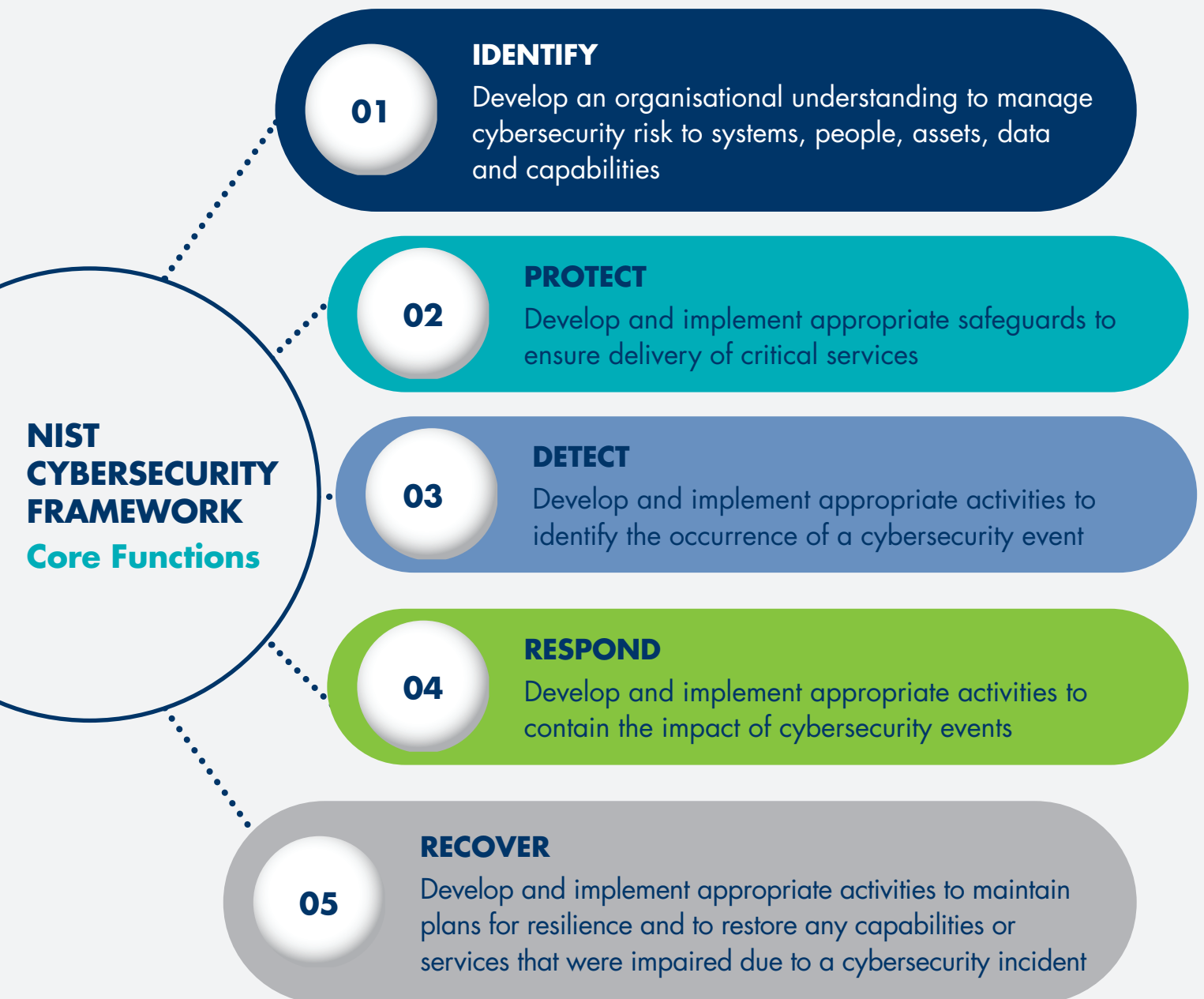
Disable location tracking on each app. A study of almost one million Android phones showed that apps regularly harvested tracking data.

The NIST Cybersecurity Framework Core Functions

It is challenging for organisations to integrate cybersecurity into their business models. However, the Framework for Improving Critical Infrastructure Cybersecurity referred to here as the NIST cybersecurity framework can assist organisations to structure and simplify the implementation of the various security controls.

NIST CYBERSECURITY FRAMEWORK
Core Functions

01
IDENTIFY
Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities

02
PROTECT
Develop and implement appropriate safeguards to ensure delivery of critical services

03
DETECT
Develop and implement appropriate activities to identify the occurrence of a cybersecurity event

04
RESPOND
Develop and implement appropriate activities to contain the impact of cybersecurity events

05
RECOVER
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

For more information, contact Information and Cyber Security Centre (ICSC):

Dr Jabu Mtsweni (jmtsweni@csir.co.za) and
Dr Zubeida Dawood (zdawood@csir.co.za)