zentera™

A Zero Trust Guide to to the NCSC Cyber Assessment Framework

October 2020

A Zero Trust Guide to the NCSC Cyber Assessment Framework

What is the NCSC?

The National Cyber Security Centre (NCSC), formed in 2016, provides information security support to organizations and enterprises in the UK.

NCSC and the NIS Directive

The NCSC supports the UK implementation of the EU NIS Directive by acting as a single point of contact for engagement with EU partners, coordinating incident response among Competent Authorities (CA), and acting as a technical authority on cyber security matters.

As part of supporting the NIS Directive, NCSC has developed a Cyber Assessment Framework to help organizations understand and adopt a holistic set of cyber security principles and best practices.

About The Cyber Assessment Framework

The Cyber Assessment Framework (CAF) provides indicators of good practices, rather than a compliance framework. It is is intended to support organizations that

- Operate within the UK Critical National Infrastructure (CNI)
- Are subject to the EU Network and Information Systems (NIS) Directive
- Manage cyber-related risks to public safety, such as Control Of Major Accident Hazards (COMAH)

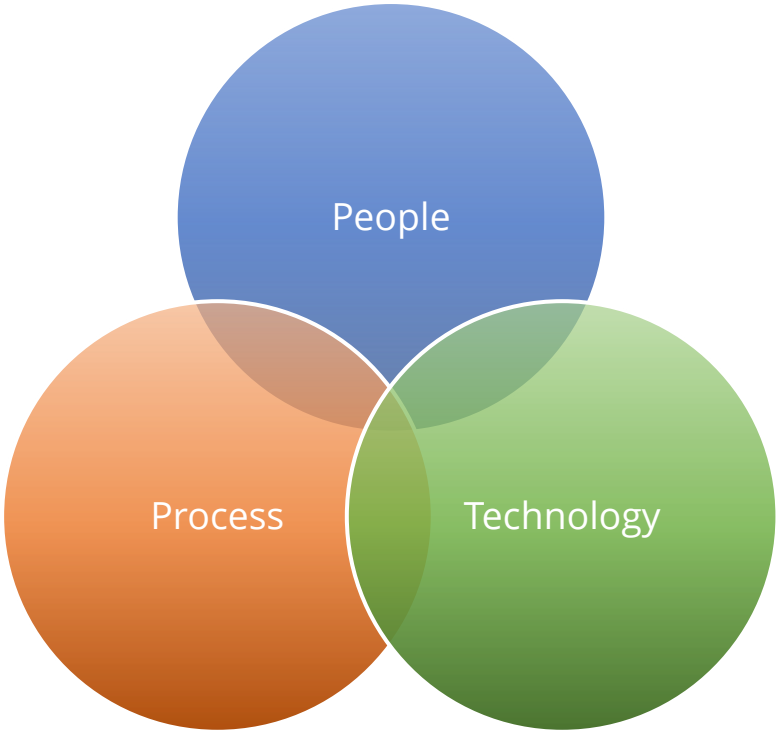
The CAF is targeted at a broader audience than the NIS Directive.

zentera™

Organizational Change Drives the Need to Modernise Cyber Security

Cyber security attacks are not new; in fact, the first computer worm was unleashed in 1988[1]. However, the increasing automation of tools and processes brought by Digital Transformation has made existing enterprises much more susceptible to cyber attacks than ever before. New risks introduced by these changes are much more pronounced for critical infrastructure, such as Energy and Utilities, where a cyber security event could have a major impact on national security and welfare.

As the nature of the operations changes, old best practices and technical solutions must be re-evaluated and re-formulated for the new reality. In reviewing their operational processes, organizations should consider three major factors: *people*, *process*, and *technology*.



With the Cyber Assessment Framework, NCSC has broken these fundamental factors into 14 *Principles* spanning 4 *Objectives*, without prescribing a specific solution. This approach enables organizations of any size and type to design a cyber security management systems appropriate to its business scope and scale.

[1] https://en.wikipedia.org/wiki/Morris_worm

What is Zero Trust?

Based on ideas first captured by the Jericho Forum in 2004, "Zero Trust" as a term was coined in 2010 by Forrester to describe a movement to replace implicit trust relationships with explicit authentication and policy-defined access control. The core tenet of Zero Trust is "never trust, always verify."

In traditional enterprise networks, the network topology creates an implicit trust relationship. Just being connected to a particular subnet automatically grants an endpoint a certain set of access rights within the corporate network. Access from point A to point B is defined by the programming of IP addresses and every router, switch, and firewall along the path, making it difficult to visualise and manage risk.

Replacing implicit trust with explicit trust surfaces any hidden security assumptions, making it easier to manage security and risk.

Zero Trust Network Access (ZTNA) is a secure method of delivering applications to users or other machines. Unlike traditional solutions, which rely on VPN and firewalls, ZTNA does not rely on the network topology at all. Instead using trust factors such as certificates, geolocation, and application fingerprinting to establish the identity of users, endpoints, and applications.

By default, no connectivity exists. When one application attempts to communicate with another, the ZTNA controller automatically performs a policy check against a centralised database, to authenticate ("are you who you claim to be?") and authorise ("are you allowed to take this action?") both ends of the connection. Only when policy checks pass is application traffic allowed to flow from end to end.

We encounter Zero Trust principles routinely in the physical world.

For example, in an airport, your access to the terminal is not assumed based on the fact that you happen to be at the airport. It's granted only after authentication (your passport), authorization (your ticket), and threat detection and mitigation (security screening).

Introducing Zentera Systems' Zero Trust Solutions

Zentera Systems flagship CoIP® Access Platform performs two key functions to help bring organizational cyber security readiness into the Digital Transformation era.

Zero Trust Network Access

ZTNA is a secure remote access method, which enables both users and machines to securely access applications inside the corporate perimeter. The corporate firewall does not need to be opened to allow the access, and the remote user or machine's access scope is limited to that granted by policy, enabling adherence to least privilege principles.

Zero Trust Micro-Segmentation and Application Segmentation

Zero Trust Micro-Segmentation protects critical applications and data in place. Applications are first cloaked from the shared network, rendering them 'invisible' to machines on the network. Whitelisted connections are then re-established using ZTNA methods, providing total control over application segmentation, whether north-south or east-west.

In contrast with other Zero Trust solutions, Zentera's ZTNA and Zero Trust Micro-Segmentation and Application Segmentation deploy on top of existing network without touching existing network and security infrastructure – either by an OS-level agent, installed on the application server, or by a gateway installed in front of the application server. This means that the existing infrastructure does not need to be upgraded or replaced to achieve dramatic reductions in the attack surface.

How Zentera's Zero Trust Helps Organizations Adapt to Change

Zero Trust with CoIP Access Platform is a critical component that helps organizations adapt to change without a complete overhaul of people, process, and technology.

People

CoIP Access Platform streamlines remote access for users, by making every access work the same way. Regardless of where a user is, ZTNA provides consistent access methods that are easy-to-use and backed by the organization's existing identity services with SSO, reducing incentives for end users to find creative "shadow IT" solutions to their IT challenges.

Zentera's ZTNA application access model enables IT teams to streamline communications with auditors, regulators, and boards of directors about *what* access is provided to *whom*, and to rapidly support end users as they onboard and use corporate applications.

Process

CoIP Access Platform enables organizations to automate repeatable processes to reduce the risk of human error. By providing centralised end-to-end control over user- and machine-access and application-based micro-segmentation that spans any datacenter, cloud, or OT environment, organizations are freed from having to coordinate activities between multiple siloed teams for day-to-day management, incident response, or compliance reporting.

Technology

CoIP Access Platform's Zero Trust represents the leading edge of cyber security – Zero Trust capabilities, created to support existing brownfield deployments without infrastructure re-engineering. Completely decoupling user access and application-based micro-segmentation from the underlying infrastructure enables an unprecedented degree of user and application mobility to support existing as well as new Digital Transformation initiatives.

Zentera CoIP Access Platform's mapping to the NCSC Cyber Assessment Framework's 14 Principles is detailed in the next section.

Zentera Zero Trust to NCSC Cyber Assessment Framework Mapping

Objective A: Managing Security Risk

Principle	Principle Description (summary)	Zentera Capabilities
A.1 Governance	Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.	Zentera supports governance efforts by converting network policies otherwise encoded in distributed routers and firewalls into simple, human readable and auditable end-to-end policies. CoIP Access Platform provides full change control logs, as well as access monitoring and the ability to detect policy drift. With Zentera Zero Trust Network Access, governance policies and processes are streamlined and made more powerful.
A.2 Risk Management	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.	Zentera's CoIP Access Platform supports risk management efforts by providing risk information to guide the assessment process. Forms of risk information include visibility into access communications, baseline network traffic, and discovery of new communications patterns and behaviors.
A.3 Asset Management	Determining and understanding all systems and/or services required to maintain or support essential functions.	Zentera tools can be used to augment asset management tools by monitoring for and discovering new assets in established segmentation and communication profiles.
A.4 Supply Chain	Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers,	Zentera Secure Access enables Zero Trust secure remote access to corporate applications for vendors and well as other external parties. With strong authentication of users, endpoints, and applications, and policy-based authorization, organizations can provide access while insulating themselves from risks that may be introduced from supplier networks.

Objective B: Protecting Against Cyber Attack

Principle	Principle Description (summary)	Zentera Capabilities
B.1 Service protection policies and processes	Defining and communicating appropriate organisational policies and processes to secure systems and data that support the operation of essential functions.	Zentera supports secure service protection practices by providing application and network security segmentation that is driven by IAM, while being simple and easy to use for users. This approach minimises attack surface in lateral attack vectors, and extends the principle of least privilege access security without encouraging users to find workarounds.
B.2 Identity and access control	Understanding, documenting and controlling access to networks and information systems supporting essential functions.	Zentera CoIP Access Platform integrates with the existing corporate IdP through SAML 2.0 to identify users with MFA; the platform identifies endpoints and applications through a variety of attributes that include geolocation, device identifiers and metadata, and certificates, to provide policy-based controls for access to essential functions.
B.3 Data security	Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions.	Zentera secures data in transit with TLS1.3 end-to-end encryption. Additionally, CoIP Access Platform cloaks critical hosts on the network, making them invisible to unauthorised accesses.
B.4 System security	Protecting critical network and information systems and technology from cyber attack.	Zentera's CoIP Access Platform defends critical network and information systems and technology with a Zero Trust approach - communications are treated with a default "deny" policy, and allowed only after passing authentication and authorization. Access control, micro-segmentation, and threat detection/prevention features help to ensure the security of application traffic.

Objective B: Protecting Against Cyber Attack (continued)

Principle	Principle Description (summary)	Zentera Capabilities
B.5 Resilient networks and systems	Building resilience against cyber attack.	Zentera enables design of resilient Zero Trust and micro-segmentation architectures, leveraging TCP/IP to provide alternate routes in the event of a service outage or attack. CoIP Access Platform can automatically quarantine endpoints to help minimise impact on service and business continuity. The platform leverages techniques such as mutual authentication and anti-tamper mechanisms to defend itself. Additionally, the platform supports multi-gigabit per-flow throughput, which can be leveraged for high-speed remote backup/restore to support stringent RPO/RTO objectives.
B.6 Staff awareness and training	Appropriately supporting staff to ensure they make a positive contribution to the cyber security of essential functions.	Zentera promotes staff awareness and compliance by simplifying compliance for administrators and end users, and by providing feedback when users attempt to circumvent the prescribed policies.

Objective C: Detecting cyber security events

Principle	Principle Description (summary)	Zentera Capabilities
C.1 Security monitoring	Monitoring to detect potential security problems and track the effectiveness of existing security measures.	Zentera platform supports monitoring various types of events that could indicate security risks, including communication policy violations, tamper detection events, and endpoint policy violations (e.g. geolocation failures). Integration with 3rd party SIEM tools enables centralised threat assessment, detection and response.
C.2 Proactive security event discovery	Detecting anomalous events in relevant network and information systems.	Zentera's Smart Discovery feature enables automatic ML-driven micro-segmentation definition, and detects anomalous network behavior and traffic.

Objective D: Minimising the impact of cyber security incidents

Principle	Principle Description (summary)	Zentera Capabilities
D.1 Response and recovery planning	Putting suitable incident management and mitigation processes in place.	Zentera platform supports incident response processes with capabilities such as auto-quarantining of anomalous systems for analysis and remediation.
D.2 Lessons learned	Learning from incidents and implementing these lessons to improve the resilience of essential functions.	Zentera CoIP Access Platform supports post-incident analysis by providing clear logs of what policies were in effect, what network activity occurred, and which trust factors were satisfied to enable remote access, pass micro-segmentation filters, or pass through threat detection.

Conclusion

The NCSC Cyber Assessment Framework provides a useful reference to help organizations evaluate their cyber security posture. By performing a gap analysis, organizations can identify concrete steps they can take to improve the overall cyber readiness, as well as communicate their progress toward their goals to boards of directors, regulators, and other stakeholders.

Zentera Systems' Zero Trust Network Access tools enable secure remote access for users and applications, and also enable application-focused micro-segmentation that enhances the security of critical applications and data.

Zentera's ZTNA tools support a transformation of an organization's security posture by:

- Providing simple policies and logs that can be understood by **people**, rather than machines
- Supporting streamlined **processes** that reduce the desire for users to implement "shadow IT" and also reduce opportunities for human error
- Delivering advanced **technology** that builds trust based on the identity of users, endpoints, and applications, rather than network topologies, supporting application and data mobility

Organizations looking to leverage the NCSC Cyber Assessment Framework should consider Zero Trust Network Access as an effective tool to close the gaps in their cyber security management systems.