DARKTRACE

Darktrace Framework Mapping:

Code of Practice Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance

Office of the Commissioner of Critical Infrastructure (Computer-system Security) Security Bureau.
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Released on 1 January 2026, Code of Practice Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance provides practical guidance for Critical Infrastructure (CI) operators and sets the baseline requirements for protecting critical computer systems (CCSs).

Rather than introducing entirely new concepts, it consolidates and formalizes expectations across:

- **Risk** management and governance
- **Asset** identification and protection
- **Access** control and remote connection security
- **Threat** detection and monitoring
- **Incident** response and recovery
- Ongoing **assurance**, audit and compliance reporting

By aligning CoP controls to real-world capabilities, the goal is not just to support compliance, but to clarify:

- Where coverage already exists
- Where compensating controls may help reduce risk
- Where operator-owned processes still remain necessary
- How security outcomes can be measured and improved over time

This document highlights the mapping between selected CoP requirements and Darktrace capabilities, illustrating where Darktrace can support asset visibility, risk-based prioritization, anomaly detection, logging, remote access monitoring, OT network security, and incident readiness. It is intended as a practical alignment guide, not as a legal interpretation of the Code or a complete mapping of all requirements.

How Darktrace helps align to the CoP

Threats facing critical infrastructure across IT, OT, IIoT, IoT, and cloud are increasing. Nation-states, insiders, and cybercriminal groups are becoming more sophisticated, using techniques such as living off the land and supply chain attacks to penetrate OT environments.

Darktrace is the most comprehensive OT security solution purpose built for critical infrastructure. By learning "normal" across IT, OT, and IoT assets, it autonomously detects, investigates, and responds to novel attacks before they disrupt operations.

Darktrace provides comprehensive asset visibility across OT, IT, IoT, and IoMT environments, supports anomaly-based detection and AI-led investigation, enables risk management beyond CVEs, strengthens governance and compliance reporting, and delivers trusted response for OT. It is designed to help organizations defend critical production systems while maintaining uptime, reduce audit fatigue and compliance costs, and mitigate risk in complex converged environments.

Darktrace brings together OT, network, endpoint, cloud, email, AI tools, and human and agent identities to unify visibility and defense across the digital estate. By learning from your unique environment, the platform helps organizations identify risk earlier, improve investigation speed, strengthen resilience, and support more effective security operations across converged IT, OT, and cloud environments.

From the official CoP: "This Code is not subsidiary legislation, nor would failure to comply with the provisions of this Code in itself constitute an offence. However, the Commissioner may issue written directions to require a CI operator to take appropriate actions (...). Failure to comply with such directions would be an offence."

NOTE: This is not a complete mapping of the all the requirements, nor is it advice for practitioners. This mapping represents aspects of the CoP which Darktrace best supports practitioners in their pursuit toward cyber resilience within the framework.

Section	Description & Requirement Summary	Darktrace Coverage
4.1	Requiring Information for Designating Critical Computer Systems	Darktrace inventories the devices seen communicating on the network and can also discover and inventory externally facing devices. Darktrace also discovers and inventories the platforms and applications of an organization. Darktrace has passive and optional active components to gather evidence of IT and OT devices, and of network services inferred from the analysis of connections and protocols.
6.2.	**Computer-System Security Risk Management Approach** - Identification, assessment, mitigation and monitoring of risks	Darktrace uses a risk-based approach to continuously map every possible attack path from the attack surface to the internal systems and prioritizes these risks with suggested mitigation. Darktrace continuously assesses and reports on risks associated with an organization's operations, assets, and people. Darktrace then identifies and prioritizes the corresponding risk response actions. Darktrace can be configured to support an organization's governance and risk management processes with varying levels of automation, reporting and/or alerting.
6.2.9	**Asset Management** - Maintain up-to-date inventories of CCSs and associated assets, including relevant hardware, software, applications, locations, and ownership information.	Darktrace inventories the devices seen communicating on the network and can also discover and inventory externally facing devices. Darktrace also discovers and inventories the platforms and applications of an organization.
6.2.10	**Access Control and Account Management** - Preventing unauthorized access and ensuring only authorized personnel can access critical computer systems (CCSs)	▪ Darktrace acts as a compensating countermeasure by detecting and alerting to many types of brute force and failed login situations from within network traffic. ▪ Darktrace can gather evidence of events which may represent malicious attempts to gain unauthorized access. ▪ Darktrace products in scope have the mechanism to enforce limitations on consecutive invalid access attempts and deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.
6.2.11	**Privileged Access Management** - Ensuring that privileged access rights of CCSs are provided only with authorization, with the principle of least privilege for administrative accounts enforced	▪ Darktrace detects and interrupts anomalous user activity including violations of least privilege and separation of duties. ▪ Darktrace products are configurable using roles-based access control (RBAC) to support segregation of duties and principle of least privilege. They support single sign-on (SSO) and multi-factor authentication (MFA), making it extremely difficult for users to misuse accounts.
6.2.18	**Remote Connection** - Implementation of suitable security measures to prevent unauthorized remote access to CCSs and their data	Darktrace identifies remote access activity and interrupts remote activity that is not permitted and/or that is deemed anomalous. Darktrace can act as a compensating countermeasure by monitoring for signs of unusual and potentially unauthorized access to information over the network, including unusual remote access sessions. Darktrace can gather evidence of unusual remote access sessions.
6.2.21	**Network Security** - Network intrusion detection system (NIDS) or a network intrusion prevention system (NIPS) at critical nodes of the CCS; log, monitor, detect and stop attacks	Darktrace detects and interrupts anomalous activity and potential malicious software for all devices within the network. Darktrace continuously monitors an organization's network both internally and externally and can alert on and interrupt unauthorized and/or anomalous activity. Darktrace continuously identifies and prioritizes an organization's digital assets, even new devices as long as they are on the network. Darktrace continuously monitors the flow of information of all of these assets.
6.2.23	**Log Management** - Record and identify the events involving CCSs that may lead to a computer-system security incident; this includes log-on attempts, use of privileged rights, changes to user access rights	Darktrace continuously monitors and logs activity including admin activity. Darktrace also supports the automated collection and analysis of log records. Darktrace includes an audit log of events relating to its own configuration by recording evidence of any auditable activities that can be identified traversing the network. It provides a central view of network activity and can serve as a compiled, time-correlated audit record to support evidence gathering. Darktrace products can export their outputs and logs to other systems via syslog, HTTP, and other supported methods for integration with SIEMs or other centralized audit trail platforms.

Section	Description & Requirement Summary	Darktrace Coverage
6.2.24	**Cloud Computing Security** - Identifying, assessing, evaluating and responding to computer-system security risks associated with the adoption of cloud computing	Darktrace correlates incidents across multiple domains like email, identity, network, cloud, endpoint and OT, consolidated by a single Self-Learning AI engine. Darktrace provides enhanced visibility over cloud-based assets, the network monitoring is performed out-of-band on separate hardware, in the Cloud and/or using virtual sensors that can be restricted by their hypervisors.
6.2.26	**Monitoring and Detection** - Mechanism to monitor the continuous operation of CCSs for detecting anomalies and potential computer-system security incidents	Darktrace's ActiveAI Security Platform provides real-time detection, autonomous response, proactive exposure management, attack surface management, and incident readiness and recovery. Darktrace uses AI to autonomously analyse 100% of events and provide information on potential targets and methods of an attack. Darktrace continuously monitors organizational systems and alerts on unusual/unauthorized activities. Darktrace leverages continuous learning to understand the normal activities for users. When a user's activity is deemed anomalous, Darktrace can alert on it and interrupt the activity. Darktrace can be used to demonstrate compliance via multiple features that support timely response: Data ingestion, analysis and initial alerting are near-real-time.
6.2.27	**Computer-System Security Training** - Formulation of a training program that delivers targeted and structured training periodically to all personnel involved in CCS operation, fostering their awareness and enabling them to fulfil their computer-system security responsibilities	Darktrace engages key users to test and educate them on their role in ensuring the security of an organization. Darktrace provides simulations to test an organization's people, process and technology, helping organisations understand their incident readiness and recovery levels. Darktrace's Cyber AI Analyst is designed to behave like a trained cyber analyst and augments the skills and bandwidth of security teams. Darktrace provides simulated incident drills to train personnel on practical incident response procedures. Simulated incidents can be used to discover and resolve issues with planned procedures.
6.3	**Obligation to conduct computer-system security risk assessments** - Identify risks to the CCSs, including the likelihood and severity, the level of risks that the CCSs can tolerate, and the required risk mitigation measures and monitoring. The computer-system security risk assessment should include a vulnerability assessment and a penetration test which, among other steps, identify security and control weaknesses.	Darktrace continuously monitors assets for known and new vulnerabilities, provides risk-based recommendations for vulnerability remediation, and autonomously implements enhanced detection and response for temporary remediation. Darktrace continuously assesses and reports the risks associated with an organization's operations, assets, and people. Darktrace identifies vulnerabilities within an organization, integrates with 3rd party vulnerability and threat intelligence feeds, and can autonomously adjust detection and response capabilities to account for vulnerable assets. Darktrace uses a risk-based approach to continuously map every possible attack path from the attack surface to the internal systems and prioritizes these risks based on impact and likelihood with suggested mitigation. Darktrace continuously monitors for threats and vulnerabilities in order to protect an organization's digital assets. Darktrace can also detect and interrupt anomalous activity further protecting digital assets.
6.5.7	**Network Security** - Plan and implement adequate network security controls on the CCSs to detect and manage malicious traffic from accessing the CCS	Darktrace detects and interrupts anomalous activity and potential malicious software for all devices within the network. Darktrace can act as a compensating countermeasure because it provides visualization of network traffic flow, which can be used to confirm the segmentation matches the intended design.
6.5.8	**Monitoring and Detection** - Define and implement policies and procedures for protecting endpoint devices against malware, taking into account (amongst others), the impact on the normal functioning of an OT system	Darktrace identifies known and unknown malware in real time without using rules or signatures. Detection is based on the attack phases including but not limited to Egress, C2 communication, lateral movement, internal reconnaissance, exploit. Darktrace analyses attachments, links and emails for signs of threat and surgically responds to the attachments, links or the entire email. Darktrace leverages continuous self-learning to understand the normal activities for users. When a user's activity is deemed anomalous, Darktrace can alert on it and interrupt the activity. Darktrace uses AI to autonomously analyze 100% of events and provide information on potential targets and methods of an attack. Darktrace leverages continuous learning to understand the normal activities for users. When a user's activity is deemed anomalous, regardless of due to malware, Darktrace can alert on it and interrupt the activity. Based on different lists, Darktrace can alert on and interrupt unwanted activity.

Section	Description & Requirement Summary	Darktrace Coverage
6.5.9	**Computer-system Security Risk Assessment** - If conducting a vulnerability assessment or a penetration test could adversely impact the normal functioning of an OT system, the CI operator should use alternative vulnerability identification activities (e.g. performing targeted vulnerability scans or penetration tests on critical peripheral nodes of a CCS) to discover computer system security weaknesses in the CCSs	▪ Darktrace acts as a compensating countermeasure by monitoring for unusual activity on the network or zone based on many data points, including but not limited to: time, session duration, location, and authentication methods. ▪ Darktrace continuously monitors assets for known and new vulnerabilities, provides risk-based recommendations for vulnerability remediation, and autonomously implements enhanced detection and response for temporary remediation. Darktrace identifies vulnerabilities within an organization, integrates with 3rd party vulnerability and threat intelligence feeds, and can autonomously adjust detection and response capabilities to account for vulnerable assets.
7.1	**Obligation to participate in computer-system security drill** - To be conducted to assess the validity and effectiveness of CI operator's emergency response plan; and assess the participating personnel's knowledge of their roles and responsibilities in responding to computer-system security incidents.	▪ Darktrace applies a comprehensive understanding of an organization's environment and data to continuously assess and optimize both human and system readiness. ▪ Darktrace can create simulated incidents that allow organizations to test a wide range of incident types. These simulations do not represent real threats; instead, they are generated using real incident telemetry and overlaid onto the organization's environment to provide highly realistic scenarios. Simulated incidents can be tracked throughout the incident interface from initial compromise through payload execution, response actions, and eventual recovery. ▪ Darktrace supports the execution of tabletop exercises by enabling organizations to select their own use cases while utilizing their own devices as participants in the exercise. ▪ Darktrace also enables participation from non-security teams by allowing organizations to predefine relevant personnel and establish a dedicated command center, such as a Microsoft Teams group or coordinated communication without exposing sensitive security information.
7.2	**Obligation to submit and implement emergency response plan** - Formulate an emergency response plan, and set out the protocol for responding to computer-system security incidents targeting CCSs. The scope of the plan should include the following: incident management; and business continuity management and disaster recovery	▪ Darktrace determines the most effective course of action to eradicate identified threats and dynamically adjusts the organization's security posture to harden against repeat or similar attacks. ▪ Darktrace generates AI-driven playbooks that adapt uniquely to the nature and severity of each incident. These playbooks prioritize containment, evidence collection, investigation, and recovery. When multiple devices are involved, Darktrace autonomously determines the optimal sequence of actions per device to maximize recovery outcomes. Dynamic playbooks are constructed based on identified threats and risks. When an incident occurs, these dynamic recovery playbooks automatically adapt response actions to the precise details of the event. Each playbook is composed of customizable Playbooklets, and each Playbooklet consists of specific Recovery Steps. Organizations can modify the strategies and descriptions of Playbooklets by managing their constituent Recovery Steps. ▪ Darktrace integrates with ticketing systems and collaboration platforms including ServiceNow and Microsoft Teams to support cross-team coordination, follow-up actions, and streamlined incident workflows. ▪ Darktrace also enables the documentation of both system-initiated and human-initiated actions within the same interface during the recovery process. This information includes which user performed which recovery step and at what date and time can be exported for comprehensive post-incident review.