

Report to the Chair and Members of the Audit Committee
27 August 2024
Status: For information

Annual Cyber Security and Information Risk Guidance for Audit Committees

1. Purpose

- 1.1 The purpose of this report is to provide the Audit Committee with continued assurances that Cleveland Police has implemented the necessary technical, physical, personnel and procedural security controls to protect its information and satisfy national Information Assurance (IA) requirements that are pertinent to government and policing.

2. Recommendations

- 2.1 It is recommended that Members note the content of the report and take assurance that the appropriate information security controls are in place.

3. Information Assurance Governance

- 3.1 The force's governance framework is broadly unchanged, including specialist IA roles including a Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs) and Information Security Manager (ISM). The substantive Data Protection Officer left the organisation and the role is being covered by the Information Governance Manager with support from the ISM.
- 3.2 The Information Management Unit (IMU) is now part of a digital data and technology (DDaT) structure, alongside ICT and Digital Services. A broad review of DDaT is being led by a T/Superintendent and the issue of the DPO post is expected to be addressed there.

The SIRO is currently DCC Victoria Fuller. The strategic risks remain

- i. loss/disclosure of paper documents;
- ii. inappropriate disclosure electronically (e.g., email, social media);
- iii. availability of critical computer systems;
- iv. loss/disclosure of removable media; and
- v. physical security of sites.

- 3.3 The Information Assurance Board was replaced by/incorporated into the Digital Data and Change (DDaC) board. This meets monthly, with a quarterly meeting specially dedicated to IMU issues.
- 3.4 The baseline e-learning training for all officers and staff remains "Managing Information" (operation and non-operational) and "Government security classification", to be repeated every two years. PowerBI dashboards enable supervisors and IMU to monitor compliance of e-learning packages. An "information security policies and guidance questionnaire" (aka "the infosec

compliance survey”) has been re-published recently to emphasise significant aspects of the policy across the whole organisation. This is also tracked via a PowerBI dashboard and is to be reported to DDaC.

- 3.5 Demand on the information security team is high. A team restructure is in progress to improve resilience and capability, although this will not improve capacity.
- 3.6 Security incidents continue to be recorded, assessed and reviewed by the ISM. Whether personal information is involved, IMU makes an assessment in relation to notifying the Information Commissioner’s Office. Critical incidents are handled by “gold” groups.

4. Compliance

- 4.1 The Force is registered with the Information Commissioner’s Office and ensures compliance with GDPR and the Data Protection Act (2018) through the duties and responsibilities of the acting Data Protection Officer.
- 4.2 Remediation from previous IT Security Health Checks (ITSHC aka ITHC) continues to improve, although some legacy issues remain outstanding. Processes have been revised and improved to assist in tracking and targeting ITHC and related issues.
- 4.3 We remain fully engaged with Police Digital Services (PDS) and the Security Assessment for Policing (SyAP) process. PDS issued a second annual report in June. This continues to highlight the high risk of ransomware. The report noted that “Since the last SIRO report in July 2023, Cleveland have made slow but steady positive progress in improving their score.”

5. Implications

- 5.1 Finance
There are no financial implications arising from the content of this report.
- 5.2 Diversity and Equal Opportunities
There are no diversity or equal opportunity implications arising from the content of this report.
- 5.3 Human Rights Act
There are no Human Rights Act implications arising from the content of this report.
- 5.4 Sustainability
There are no sustainability implications arising from this report.
- 5.5 Risk
The risk of ransomware attack remains incorporated in the existing “availability of critical computer systems” strategic risk.