CARDIFF SCHOOL OF TECHNOLOGIES

4D Digidol | Data | Dylunio | Dyfodol

Cardiff Metropolitan University	
Cardiff School of Technologies	
Academic Year: 2025/2026	
Term: 1	
Module Name: Information Security	
Module Code: SEC7000	
Module Leader: Dr Liqaa Nawaf	
MSc Programme: Advanced Cyber Security	
Assignment Title: Information Security Assignment	
Student Name: Sid Ali Bendris	**Student ID: 20238021**

Contents

Chapter

Table of figures

Chapter 1

1.1 Operationalising Data Protection by Design & Default (DPbD)

For this project, Data Protection by Design and Default (DPbD) must be treated as an engineering and governance requirement, not a “compliance afterthought”. The proposed solution combines CCTV, facial recognition technology (FRT) and a centralised contact tracing capability, which raises the likelihood of high-impact harm. DPbD therefore needs to be embedded from the earliest requirements stage and maintained through deployment and ongoing operation, as required by Article 25 UK GDPR. Operationally, the organisation should implement DPbD through a privacy-aware secure development lifecycle (SDLC) with defined “gates” and accountable owners. At the requirements stage, the controller should explicitly document: (1) the precise purposes of processing, (2) the lawful basis, and (3) whether any special category processing is involved (notably biometrics when FRT is used for identification). The organisation should then run a Data Protection Impact Assessment (DPIA) early and treat it as a living document that is updated when the design changes for example adding new camera zones, changing retention, or onboarding a new vendor. This aligns with the ICO’s expectation that DPbD is part of accountability and governance rather than an optional add-on.

At the design stage, DPbD should translate into concrete defaults that enforce data minimisation and purpose limitation. For example: limit camera coverage to strictly necessary zones; avoid continuous identification where detection or counting would suffice; restrict the FRT pipeline so that biometric matching only occurs when a tightly defined trigger condition is met; and design data flows to separate identifiable records from operational analytics wherever possible. Article 25(2) requires that “by default” only the personal data necessary for each purpose are processed so the system’s default configuration should implement minimal collection, minimal retention, and minimal access as the baseline, with any expansion requiring documented approval and risk justification. At the build and test stages, DPbD should be evidenced through privacy/security requirements that become testable controls: role-based access control with least privilege; MFA for administrative roles; encryption in transit and at rest with managed keys; immutable audit logs; and privacy test cases that would include verifying that non-authorised staff cannot search by name/face, and that access to footage is logged, reviewed, and tied to a legitimate task. The ICO’s CCTV and video surveillance guidance emphasises handling people’s information rights in video contexts like access requests, so the design must also support efficient retrieval, redaction where appropriate, and controlled disclosure workflows.

Finally, DPbD must continue into operations: continuous monitoring for misuse, periodic access reviews, retention enforcement, vendor assurance, and change control to prevent function creep. The organisation should also align with established guidance on video processing, which stresses proportionality and careful assessment of necessity when deploying video-based systems, especially where more intrusive “smart video” capabilities are involved.

DPbD requirement / principle	What it means in this system (CCTV + FRT + centralised tracing)	Privacy/security controls (technical defaults)	Organisational controls (process & governance)	Evidence / audit artefacts (what you can show)
"By design" (integrate DP throughout processing)	DP is engineered from requirements → deployment, not bolted on later.	Privacy requirements as non-functional requirements (NFRs); threat modelling + privacy misuse cases baked into design.	SDLC "privacy gates" (design review sign-off before build; security/privacy sign-off before go-live).	SDLC checklists; threat model; design review minutes; privacy test results.
"By default" (only necessary data for each purpose)	Default settings minimise collection, access and retention, unless justified.	Default: minimal fields in tracing DB; least-privilege roles; restricted search features; shortest retention as baseline.	Change control required to expand data fields, retention, or access scope (documented justification + re-assessment).	Configuration baseline; RBAC matrix; retention schedule; change requests + approvals.
Data minimisation	Avoid capturing/processing more than needed (especially biometric identifiers).	Camera zoning & masking; avoid always-on identification; use detection/counting when ID isn't required; collect only essential tracing attributes.	Purpose statements and "must-have vs nice-to-have" review with DPO; periodic minimisation reviews.	Camera coverage map; masking config; data dictionary; minimisation review logs.
Purpose limitation & anti–function creep	Prevent repurposing into general surveillance, HR monitoring, policing without lawful basis.	Purpose-bound access controls (use-case tags); query restrictions; separation of duties between public health ops and admin.	Clear policy: permitted purposes; approval workflow for any new purpose; vendor contract clauses preventing secondary use.	Policy document; access logs showing "purpose tags"; vendor DPIA annex + contract clauses.
Pseudonymisation & separation of identifiers (PETs)	Reduce harm if the central store is breached; make linkage harder.	Tokenisation/pseudonym IDs for contact tracing; split databases (identifiers vs exposure events); join keys protected in KMS/HSM.	Key management policy; restricted "re-identification" roles; two-person rule for re-ID operations.	Architecture diagram; KMS/HSM config; key rotation records; re-identification approval logs.

DPbD requirement / principle	What it means in this system (CCTV + FRT + centralised tracing)	Privacy/security controls (technical defaults)	Organisational controls (process & governance)	Evidence / audit artefacts (what you can show)
Transparency & user control	People must understand what's happening (especially for CCTV/FRT contexts).	Layered privacy notices (QR codes/signage + app notice); consent/notice mechanisms where relevant; UI for access requests processing.	Communications plan; DSAR workflow; staff training on handling requests/complaints.	Privacy notices; signage photos; DSAR procedure; training completion logs.
Access limitation (least privilege)	Strictly control who can view footage, run searches, or manage biometric systems.	RBAC; MFA for privileged roles; PAM for admin actions; time-bound access; strong authentication.	Access approval & quarterly reviews; joiner-mover-leaver process; segregation of duties.	RBAC matrix; IAM policies; access review reports; PAM session logs.
Integrity & confidentiality (security built-in)	High-value sensitive dataset requires layered security across endpoints, networks, data stores.	Encryption in transit/at rest; secure API gateway; segmentation; EDR; immutable logs; anomaly detection on admin queries.	Incident response integration; security monitoring playbooks; supplier assurance for CCTV/FRT vendors.	Encryption/KMS evidence; network diagrams; SIEM alerts; vendor security assessment results.
Storage limitation & secure deletion	Ensure footage/contact-tracing data isn't retained "just in case".	Automated retention enforcement; deletion workflows; cryptographic erasure for keys; WORM logs for audit trails (not raw data).	Retention policy aligned to purpose + risk; documented exceptions with expiry; periodic retention compliance audit.	Retention policy; deletion logs; audit reports; exception register.
DPIA as a living control	FRT + surveillance is likely high risk; DPIA drives design choices and mitigations.	DPIA outputs become requirements (controls to implement + tests to pass).	DPIA completed early; reviewed on changes (new zones, new model/vendor, new data fields).	DPIA document; risk register; mitigation tracking; change-triggered DPIA updates.

DPbD requirement / principle	What it means in this system (CCTV + FRT + centralised tracing)	Privacy/security controls (technical defaults)	Organisational controls (process & governance)	Evidence / audit artefacts (what you can show)
Accountability & auditability	Ability to prove compliance, not just claim it.	Full audit trails: who accessed what, when, why; tamper-evident logging; monitoring for policy violations.	Governance board (DPO + security + legal); KPIs (access review completion, retention compliance, incident drills).	Audit logs; governance meeting notes; KPI dashboards; internal audit findings and remediation.

Table 1 DPbD operationalisation table

1.2 Comparative analysis: ISO/IEC 27001, Cyber Essentials, NIST CSF and COBIT vs UK GDPR

The UK GDPR is principles-led, requiring organisations to demonstrate that processing is lawful, fair and transparent, limited to specified purposes, minimised, accurate, time-limited, and protected by integrity/confidentiality, with accountability sitting above all other principles. In this project deploying CCTV with facial recognition technology (FRT) and a centralised contact-tracing capability these principles must be translated into operational safeguards that reduce surveillance harms and security risks while supporting legitimate public health objectives. The ICO notes that FRT typically involves biometric data and, in most cases, it sees, special category personal data, raising the bar for governance, proportionality, and safeguards. Security and governance frameworks such as ISO/IEC 27001, Cyber Essentials, NIST CSF 2.0, and COBIT 2019 help convert the GDPR's high-level obligations into actionable controls and management practices, but they do not "replace" GDPR compliance. Instead, they provide structured mechanisms that strongly support the GDPR's integrity/confidentiality and accountability requirements, while GDPR adds specific privacy duties such as transparency, lawful basis, data subject rights, and DPIAs.

UK GDPR principle (Art. 5)	**ISO/IEC 27001 (ISMS)**	**Cyber Essentials**	**NIST CSF 2.0**	**COBIT 2019**
(a) Lawfulness, fairness, transparency	**Partial** - supports governance, policies, evidence, but doesn't decide lawful basis/transparency content	**Limited** - technical baseline only	**Partial** - "Govern" helps governance, but not lawful basis/notice	**Partial** - governance/decision rights, but not GDPR lawful basis/notice
(b) Purpose limitation	**Partial** - scope definition, policies, change control can constrain use	**Limited**	**Partial** - "Govern/Identify" supports documenting context/scope	**Strong** - enterprise governance helps prevent function creep via objectives, oversight and assurance
(c) Data minimisation	**Partial** - risk-based design + access control supports minimisation, but GDPR defines "necessary"	**Limited**	**Partial** - encourages inventory and risk-informed controls, not minimisation decisions	**Partial** - governance can enforce minimisation decisions and approvals

UK GDPR principle (Art. 5)	**ISO/IEC 27001 (ISMS)**	**Cyber Essentials**	**NIST CSF 2.0**	**COBIT 2019**
(d) Accuracy	**Partial** - quality management in processes and controls, but not accuracy obligations for biometric matching	**Limited**	**Partial** - risk mgmt + monitoring can detect issues, but not "accuracy" principle itself	**Partial** - metrics and assurance can enforce accuracy governance
(e) Storage limitation	**Strong** - documented retention, secure deletion, auditability via ISMS controls	**Limited**	**Partial** - "Protect/Recover" supports resilience; retention needs GDPR policy	**Partial** - governance can enforce retention KPIs, audits
(f) Integrity & confidentiality (security)	**Strong** - security controls + continual improvement; strong evidence trail	**Strong (baseline)** - 5 technical controls reduce common attacks	**Strong** - outcomes across Protect/Detect/Respond/Recover	**Strong (governance)** - ensures security is managed, measured, assured
Accountability	**Strong** - ISMS provides governance, documentation, audit readiness	**Partial** - can evidence baseline controls, but limited governance coverage	**Strong** - "Govern" function explicitly supports organisational governance outcomes	**Strong** - formalises decision rights, KPIs/KRIs, assurance and oversight

Table 2 Mapping UK GDPR principles to ISO 27001, Cyber Essentials, NIST CSF 2.0, and COBIT 2019

ISO/IEC 27001 provides the most direct route to proving GDPR-aligned security and accountability at an organisational level through an Information Security Management System (ISMS). ISO describes ISO/IEC 27001 as the best-known ISMS standard and emphasises establishing, implementing, maintaining, and continually improving an ISMS. This is valuable for this project because an ISMS forces formal scope definition such as camera network, FRT pipeline, tracing database, risk assessment, risk treatment, and continuous improvement supporting GDPR's accountability principle through documented, repeatable governance rather than ad-hoc security. ISO 27001's Annex A control set (commonly referenced as 93 controls in the 2022-aligned structure) provides a control catalogue that directly supports confidentiality/integrity outcomes (access control, cryptography, supplier security, logging, incident management, business continuity). For a surveillance/contact-tracing system, ISO 27001 is especially helpful for supply-chain assurance (CCTV/FRT vendors), controlled access to sensitive biometric processing, incident response, and auditable security governance.

Cyber Essentials is best understood as a baseline hygiene standard rather than a comprehensive governance or privacy framework. The NCSC describes it as a government-backed certification helping organisations protect data from cyber attacks, and the scheme documentation sets out five core technical control areas for example firewalls, secure configuration, security update management, user access control, malware protection. In practice, Cyber Essentials helps demonstrate that common, preventable weaknesses are addressed-important where endpoints, admin consoles, or remote access could expose CCTV/FRT infrastructure or the central tracing database. However, it does not, by itself, address higher-order GDPR needs such as lawful basis for biometric processing, proportionality/necessity assessments, transparency and rights handling, or function creep governance. Therefore, Cyber Essentials is best positioned as a "minimum bar" within a broader governance model.

NIST CSF 2.0 offers a strong operational structure for managing cybersecurity risk through its six core functions: Govern, Identify, Protect, Detect, Respond, Recover. The addition/explicit emphasis on Govern is particularly relevant for GDPR accountability because it encourages clear decision-making, risk ownership, policies, and oversight exactly what is required to manage high-risk surveillance processing responsibly. In this project, NIST CSF 2.0 can be used to create a pragmatic "security operating model": (1) Govern-define policies, oversight, and risk appetite; (2) Identify asset inventory for cameras, FRT components, cloud/on-prem data stores, data flows; (3) Protect hardening, encryption, access control; (4) Detect-monitoring, alerting for suspicious access/search behaviour; (5) Respond tested incident handling; (6) Recover resilience and continuity. NIST CSF is not a privacy compliance framework, but it is an effective scaffold to implement and measure the security side of GDPR (integrity/confidentiality) and to show continuous risk management.

COBIT 2019 complements the above by focusing on enterprise governance of information and technology, ensuring security and privacy requirements are driven by leadership objectives, measured, and assured. ISACA characterises COBIT 2019 as including a core model with 40 governance and management objectives, and supporting components such as processes, organisational structures, policies, and information flows. This is particularly useful for preventing "privacy theatre" in high-risk systems: COBIT pushes you to clarify who evaluates and directs risk decisions, how performance is monitored, and how assurance is obtained. For CCTV/FRT and centralised contact tracing, COBIT strengthens GDPR accountability by formalising ownership (controller/processor responsibilities), performance metrics (e.g., access review completion, DPIA updates on change), and auditability (internal assurance and reporting). A critical comparison across the four frameworks shows a consistent pattern: security frameworks strongly support GDPR's integrity/confidentiality principle, but GDPR extends beyond security into legal and rights-based protections. The ICO's GDPR principles guidance places transparency, purpose limitation and data minimisation at the heart of lawful processing. In other words, you can be “secure” while still being non-compliant if you collect too much data, retain it too long, expand purposes without justification, or deploy biometrics without the correct lawful basis and safeguards. This is especially important for FRT: ICO guidance highlights that biometric recognition demands careful compliance planning, including lawful basis, DPIA consideration, and risk analysis of errors and discrimination.

GDPR obligation / risk area	**Why frameworks don’t fully cover it**	**What you implement (GDPR-specific controls)**	**Framework(s) that best support delivery**
Lawful basis + special category condition for biometric recognition	Security/governance frameworks don’t determine lawful basis or special category conditions	Decide lawful basis + special category condition; document rationale; ensure alternatives/opt-out where appropriate; keep records	COBIT (governance), ISO 27001 (documented management system) but legal decision is GDPR-led
Necessity & proportionality for CCTV/FRT (avoid surveillance creep)	Frameworks focus on “how to secure”, not “should we do this / is it proportionate”	Necessity/proportionality assessment; strict purpose statements; approval gates for any new use; periodic re-justification	COBIT (decision rights/assurance), NIST CSF “Govern” (risk governance)
DPIA lifecycle for high-risk processing	DPIAs are a GDPR accountability requirement, not a security standard requirement	DPIA completed pre-deployment; updated on change; DPO input; escalation if residual high risk	ISO 27001 (risk treatment evidence), NIST CSF (risk process structure)
Transparency (privacy notices, signage, clear comms)	Frameworks don’t specify transparency content, signage, or rights messaging	Layered privacy notice + CCTV/FRT signage; clear explanation of purposes, retention, rights, contact channels	COBIT (communications governance), ISO 27001 (document control)
Individual rights (access/erasure/objection etc.)	Frameworks don’t define rights workflows or statutory response duties	DSAR workflow; identity verification; retrieval + redaction process for footage; erasure/retention exception handling	ISO 27001 (process control), COBIT (service management/assurance)
Fairness/accuracy risks in FRT (bias, misidentification)	Frameworks don’t require fairness testing or model performance governance	Accuracy thresholds; bias testing; human-in-the-loop for high-impact outcomes; error escalation; continuous evaluation	COBIT (governance/metrics), NIST CSF (govern + detect/respond monitoring discipline)

GDPR obligation / risk area	Why frameworks don’t fully cover it	What you implement (GDPR-specific controls)	Framework(s) that best support delivery
Data minimisation by default (Article 25)	Frameworks don’t impose “minimum necessary by default” as a legal default rule	Default minimised collection, retention and access; design constraints (eg zoning/masking); strict access + query restrictions	ISO 27001 + NIST CSF support implementation, but the “default-minimum” requirement comes from GDPR
Breach reporting obligations & regulator engagement	Frameworks cover incident response, but not the GDPR legal reporting thresholds/content	GDPR breach assessment workflow; decision tree; evidence pack; regulator/individual notification procedure where required	NIST CSF (Respond/Recover), ISO 27001 (incident mgmt controls)

Table 3 Key GDPR gaps not fully covered by the frameworks, and how you close them

Bringing these approaches together, a robust strategy for this project is an integrated compliance and security model:

- GDPR (and DPbD) as the compliance “north star” define lawful purposes, minimisation rules, retention limits, transparency mechanisms, and rights handling, with DPbD requirements under Article 25 embedded into design and defaults.
- ISO/IEC 27001 as the assurance backbone use the ISMS to implement governance, risk assessment/treatment, supplier assurance, incident management and continual improvement over the full system scope.
- NIST CSF 2.0 as the operational security roadmap organise day-to-day security outcomes and maturity improvements across Govern Recover, ensuring monitoring and resilience are continuous rather than one-off.
- Cyber Essentials as the baseline “anti-common-attacks” control set ensure the most common internet-based weaknesses are systematically addressed across endpoints and infrastructure supporting CCTV/FRT/tracing.
- COBIT as the governance overlay ensure leadership accountability, clear decision rights, KPIs/KRIs, and assurance mechanisms that demonstrate ongoing compliance and effective risk management over time.

Overall, the most defensible approach is to treat GDPR as defining what must be protected and why, while ISO/NIST/Cyber Essentials/COBIT define how protection and governance are executed, measured, and evidenced. This blended approach is particularly necessary in high-risk biometric surveillance contexts, where the ICO expects strong safeguards, clear necessity/proportionality reasoning, and demonstrable accountability through DPIAs and governance artefacts.

1.3 Technical and organisational mechanisms for security implementation, incident response, and reporting

Given the sensitivity and scale of the proposed solution (CCTV, facial recognition and a centralised contact-tracing architecture), security must be implemented as a layered defence-in-depth model supported by clear operational governance. The assessment brief expects this section to cover layered security controls, real-time detection, forensic investigation, escalation, and breach notification, aligned to NIST SP 800-61, ISO/IEC 27035, and UK GDPR Article 33. At the technical layer, controls should be applied across endpoints, networks, identities, applications and data. First, identity must be treated as the primary control plane: implement role-based access control (RBAC), least privilege, multi-factor authentication for privileged roles, and privileged access management for administrative actions (including recording/admin session logging). Second, protect data flows and storage using encryption in transit (TLS) and encryption at rest, with robust key management. Third, reduce blast radius through network segmentation: isolate camera networks, facial recognition processing components, admin consoles, and the central tracing database into separate security zones with tightly controlled east–west traffic. Fourth, harden and maintain systems through secure configuration baselines, patching, vulnerability management, and secure API gateways particularly important where third-party CCTV/FRT components are integrated. For real-time threat detection, telemetry must be designed-in rather than retrofitted. Centralise logs from identity systems, admin consoles, databases, and application layers into a monitoring capability (e.g., SIEM) and implement detections tailored to this system's abuse cases: unusual administrative access, bulk searches, anomalous face-search patterns, repeated failed logins, unexpected data exports, or access outside approved hours/locations. This monitoring layer is also the foundation for forensic readiness ensuring events are timestamped, integrity-protected, and retained long enough to investigate incidents without creating unnecessary privacy risk. The incident response capability should follow established lifecycle guidance. NIST SP 800-61 structures incident handling into Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-Incident Activity, emphasising that incident response must be planned and exercised before an incident occurs. ISO/IEC 27035-1 similarly describes a structured approach for preparing for, detecting, reporting, assessing, responding to incidents, and applying lessons learned.

In practice, this means having:

1. Defined incident categories and severity levels (including privacy breaches and insider misuse).
2. An evidence-handling process (chain of custody, forensic imaging procedures, secure storage of evidence).
3. Playbooks for common scenarios (credential compromise, ransomware, unauthorised access to CCTV footage, database exfiltration).
4. Links to business continuity (backup strategy, recovery priorities, tested DR)

Severity level	Typical triggers in this system	Immediate actions (first response)	Primary owner (operational)	Escalation & supporting roles	External reporting / notification	Target timeline
SEV 1 Critical (Confirmed or imminent major harm)	Confirmed exfiltration of tracing DB / biometric templates; ransomware impacting core services; active unauthorised admin access to FRT/CCTV or mass footage export; insider misuse with evidence of high impact	Activate Incident Response (IR); isolate affected systems (network segmentation blocks); disable compromised accounts; preserve evidence (logs, snapshots); begin impact scoping; start breach log	Incident Manager (SOC/IR lead)	Immediate: CISO/Head of IT Security; DPO; Legal; Senior leadership. Comms lead on standby for statements	If personal data breach meets threshold, notify ICO without undue delay and where feasible within 72 hours of awareness; consider notifying individuals if high risk	0–1 hr: containment started. <4 hrs: exec/DPO/legal engaged. <24 hrs: initial breach risk assessment. ≤72 hrs: regulatory notification if required (ICO)
SEV 2 High (Material impact / likely reportable)	Large-scale unauthorised access to footage/face-search features (no confirmed exfil yet); compromise of privileged credentials; suspected data export; major integrity issue (tampering with tracing records)	Contain (block access, rotate keys); force MFA reset; snapshot systems; begin forensic triage; verify what data was accessed; tighten monitoring rules	Incident Manager + Technical Lead (IAM/Infra/App)	Within hours: DPO + Legal assess reportability; Business owner (Public Health Ops) informs operational impacts; Comms lead prepares internal message	Likely ICO notification depending on risk; document decision either way; prepare info required for regulator notification	0–2 hrs: containment & access lockdown. <8 hrs: initial forensics + data impact statement. <24 hrs: draft regulator pack (if notifiable) (ICO)
SEV 3 Medium (Contained	Malware detected on a single endpoint; minor misconfiguration	Fix + contain; patch/harden; verify logs for lateral	SOC lead / IT Ops lead	Security manager informed; DPO consulted if	Usually not externally reportable unless	Same day: contain + remediate. <48 hrs: root cause + lessons

Severity level	Typical triggers in this system	Immediate actions (first response)	Primary owner (operational)	Escalation & supporting roles	External reporting / notification	Target timeline
incident, limited scope)	exposing a service internally; small number of suspicious access attempts; CCTV device compromise attempt blocked	movement; reset impacted credentials; update detection rules		personal data exposure is possible; Service owner notified	risk threshold met; always record and evidence the decision	learned actions logged (ICO)
SEV 4 Low (Event / near miss)	Port scan; blocked brute-force attempts; phishing email reported; policy breach with no data exposure; minor CCTV outage with no evidence of compromise	Triage; record; tune controls; user guidance/training if needed	SOC / Service desk	Inform IT security if pattern repeats; optional DPO if any data exposure suspicion	No external reporting; maintain audit trail and trend analysis	<24 hrs: close ticket; weekly/monthly: trend review
SEV 5 Informational (Monitoring only)	Benign alerts, false positives, routine admin activity confirmed legitimate	Document outcome; improve detection quality	SOC	None unless it indicates emerging risk	None	As needed

Table 4 Incident severity classification, escalation and reporting matrix (for CCTV/FRT + centralised contact tracing)

Finally, incident reporting must be legally compliant. Under UK GDPR Article 33, where a personal data breach is notifiable, the controller must notify the supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it. If the breach is likely to result in a high risk to individuals' rights and freedoms, Article 34 requires communication to affected individuals without undue delay. The ICO's breach guidance reinforces the 72-hour expectation and highlights that if reporting is delayed, reasons should be documented. Therefore, the organisation should maintain a breach log, define the "awareness" trigger, and embed a rapid assessment process (scope, affected data types, risk to individuals, containment actions) to support timely, evidence-based reporting decisions.

Chapter 2

2.1 Incident overview, exploited vulnerability (CVE) and organisational impact/losses

This section examines the CL0P-branded extortion campaign targeting organisations running on-premises Oracle E-Business Suite (EBS), linked to exploitation of a critical zero-day vulnerability later tracked as CVE-2025-61882. Threat intelligence reporting indicates intrusions began months before public disclosure, with successful compromises enabling data theft and subsequent "name-and-shame" style extortion pressure.

Timeline

- July–August 2025: Suspicious activity observed against EBS environments; exploitation assessed as occurring as early as 9 Aug 2025 (and possibly earlier signals in July).
- 29 Sep 2025: Multiple organisations receive extortion emails claiming EBS compromise and data theft.
- Early Oct 2025: Security vendors and national agencies issue alerts; Oracle publishes a dedicated security alert identifying CVE-2025-61882 and its impact.
- Oct–Nov 2025: CL0P-associated infrastructure and leak-site activity expands; public reporting indicates dozens of alleged victims and significant exfiltrated datasets.

Vulnerability analysis

Oracle's security alert states CVE-2025-61882 affects Oracle E-Business Suite, is remotely exploitable without authentication, and if exploited may enable remote code execution (RCE). This combination (pre-auth + network reachable + RCE) is particularly dangerous for enterprise systems commonly exposed through web interfaces and integrated with core business data. Independent technical write-ups and threat intelligence summaries link CVE-2025-61882 to Oracle EBS Concurrent Processing / BI Publisher Integration (a subsystem that can interact with reports, documents, and data sources), which helps explain why attackers prioritised it for large-scale data access and exfiltration rather than purely disruptive ransomware encryption. Multiple defenders assessed the campaign as "mass exploitation" focused on data theft for extortion, consistent with CL0P's established playbook of exploiting widely used enterprise software and then monetising stolen data. From a defender's perspective, the key technical lesson is that internet-facing ERP components represent a high-value, high-impact attack surface. Once pre-auth RCE is achieved, attackers can pivot to credential access, database connectivity, report repositories, and file stores that often contain HR, finance, procurement, and identity data creating immediate confidentiality and compliance exposure.

Organisational impact and losses

Evidence from threat intelligence and reporting indicates the primary impact across affected organisations was confidentiality loss through exfiltration of large volumes of data, followed by extortion demands and the threat of publication. Public reporting in November 2025 noted that CL0P actors named nearly 30 alleged victim organisations on their leak site, illustrating the scale and reputational leverage of the campaign.

The losses associated with this type of incident typically fall into four categories:

1. Operational disruption and recovery cost: Even where attackers focus on theft rather than encryption, organisations often must take systems offline to investigate, rotate credentials/keys, restore trusted baselines, and implement emergency patches incurring downtime and remediation costs.
2. Regulatory and legal exposure: Exfiltration from an ERP/contact repository can include personal data (employees, contractors, customers). In UK/EU contexts, this can trigger incident governance obligations (risk assessment, documentation, and potentially regulator/individual notifications depending on risk).
3. Direct financial loss/extortion pressure: Reuters reported extortion demands in this campaign could range into multimillion dollar levels, reflecting the value of ERP datasets and the business impact of potential exposure.
4. Reputational damage and secondary fraud risk: Public naming on leak sites can harm trust and create follow-on risks such as credential stuffing, phishing using stolen documents, or identity/banking fraud if payroll or HR records are exposed. For example, one widely reported victim case (Korean Air's catering/duty-free unit) was described as involving tens of thousands of employee records and very large data volumes allegedly leaked, illustrating how ERP-driven breaches can scale quickly.

Overall, CVE-2025-61882 represents a modern, high-severity "enterprise application zero-day" scenario where pre-auth compromise of a core business platform enabled rapid, scalable intrusions and high-impact data theft making it an ideal case study for analysing attacker behaviour, control failures, and risk-based mitigations in Sections 2.2 and 2.3.

2.2 Critical evaluation of attacker methods (TTPs) and defensive countermeasures

This campaign is best characterised as data-theft extortion enabled by mass exploitation of an internet-facing enterprise application, rather than "traditional ransomware-first" disruption. Oracle confirmed CVE-2025-61882 as an unauthenticated, remotely exploitable flaw that can lead to remote code execution, which creates a high-likelihood initial access path wherever Oracle E-Business Suite (EBS) services are exposed over HTTP. The NVD entry highlights the vulnerability effects supported EBS versions 12.2.3–12.2.14, has CVSS 9.8, and can enable takeover of Oracle Concurrent Processing supporting why attackers prioritised it as a scalable, high-impact entry point.

Initial access and social engineering "amplification". Mandiant/GTIG describe a two-part operation. The first was months of intrusion activity against EBS environments, and the second was a high-volume extortion email campaign beginning 29 September 2025, aimed at executives and designed to rapidly monetise stolen data. Critically, the extortion emails were sent from hundreds or thousands of compromised third-party email accounts, with Mandiant assessing these credentials were likely sourced from infostealer logs to bypass spam controls and increase legitimacy. This method is effective because it separates "access operations" from "monetisation operations" even if defenders block exploitation, the later email wave pressures organisations into paying based on fear and uncertainty.

Execution, persistence, and payload staging within EBS. Mandiant reports the actor used a multi-stage Java implant framework and highlights that payloads were stored directly in the EBS database (specifically advising defenders to hunt for malicious templates in tables such as XDO_TEMPLATES_B and XDO_LOBS). This is a notable technique because it uses the target platform's own data stores as a staging mechanism, complicating detection (malicious artefacts may appear as "application content" rather than obvious binaries). It also suggests that "patching alone" is insufficient once compromise occurs defenders must assume persistence or malicious artefacts may remain even after the vulnerable entry point is closed.

Discovery, collection, and exfiltration. While public write-ups vary on the full internal chain, Mandiant states that in some cases the threat actor successfully exfiltrated significant amounts of data from impacted organisations, and substantiated extortion claims by providing legitimate file listings from victim EBS environments.

This aligns with the typical extortion model: quickly identify high-value repositories (ERP documents, BI Publisher outputs, HR/finance artefacts), stage collections, and exfiltrate to enable leverage often with minimal interest in long-term stealth once data theft is complete. Why these methods worked. Three systemic issues emerge. First, attack surface exposure: public-facing EBS components create a single point of catastrophic failure when a pre-auth RCE appears. Second, patch latency and version lifecycle risk: national guidance (NHS England) warns that "sustaining support" or end-of-life EBS releases no longer receive security updates and should be treated as vulnerable indicating that upgrade debt materially increases exploitability windows. Third, detection gaps: without application-aware monitoring (e.g., database template hunting, unusual report/template creation, abnormal admin queries), platform-native persistence can remain invisible.

Defensive countermeasures

1. Emergency patching + exposure reduction (Prevent initial access). Apply Oracle's emergency patches immediately and prioritise removing EBS from direct internet exposure (VPN/Zero Trust access, allowlisting, WAF rules where feasible). Oracle explicitly directs customers to apply patches for CVE-2025-61882. NHS England similarly assesses further exploitation as highly likely and instructs rapid patching and compromise hunting. (Framework mapping: ISO 27001 change/patch governance; NIST CSF Protect.)

2. Compromise hunting and eradication (Assume breach). Follow Mandiant's guidance to hunt for malicious content stored in the EBS database (e.g., suspicious template creation patterns and XDO_* table anomalies) and treat "patch applied" as the start of the end of incident response. (Framework mapping: NIST CSF Detect/Respond; ISO 27001 logging/monitoring and incident management.).

3. Least privilege, segmentation, and credential hardening (Limit blast radius). Enforce strict RBAC for EBS administration, isolate EBS application tiers from broader corporate networks, and protect database and service accounts (rotation, vaulting, MFA where possible). This reduces post-exploit lateral movement and restricts access to high-value ERP repositories once an application is compromised. (Framework mapping: Cyber Essentials user access control + secure configuration baseline; ISO 27001 access control; NIST CSF Protect.)

4. Telemetry and detection engineering (Reduce dwell time and theft). Centralise EBS logs, database audit logs, and admin activity into SIEM; alert on unusual report/template creation, bulk document enumeration, anomalous executive-targeted extortion themes, and abnormal data exports. Mandiant's emphasis on database-resident payloads makes application-aware

detections a priority. (Framework mapping: NIST CSF Detect; COBIT oversight through measurable KPIs/KRIs.).

5. Governance controls to prevent “extortion leverage”. Establish executive-facing playbooks for extortion emails: verification steps, legal/DPO escalation, communications governance, and evidence collection. Mandiant highlights the campaign’s executive targeting and the use of stolen third-party email accounts to increase credibility. (Framework mapping: COBIT governance objectives; NIST CSF Govern/Respond.).

In conclusion, the most effective defence is a combined approach: reduce exposure, patch rapidly, hunt for platform-native persistence, and engineer detections that understand EBS-specific artefacts, while ensuring governance pathways exist to handle extortion pressure without rushed, uninformed decisions.

2.3 Risk assessment and mitigation strategy

To translate lessons from the Oracle EBS / CVE-2025-61882 extortion campaign into actionable controls, a risk assessment was performed using a simple Likelihood (1-5) × Impact (1-5) model, where Risk Score = L×I and ratings are grouped as Low (1–5), Medium (6–10), High (11–15), Critical (16–25). The focus is on risks consistent with the campaign: pre-auth RCE of internet-facing EBS, platform-native persistence, and large-scale data exfiltration for extortion.

Asset type	**Primary threat scenario (linked to the case)**	**Key vulnerability/weakness**	**L**	**I**	**Score**	**Targeted mitigation**
Internet-facing Oracle EBS (web/app tier)	Pre-auth RCE via CVE-2025-61882	Exposure to internet + patch latency; weak compensating controls	5	5	25 Critical	Emergency patching, remove direct exposure, WAF/allowlisting, upgrade out of unsupported versions
EBS database + BI Publisher templates/content	Payload persistence & staging in DB (e.g., template tables)	Insufficient DB auditing; weak integrity monitoring	4	5	20 Critical	Threat hunting per Mandiant indicators; DB audit logging; integrity checks; restrict template authoring
Privileged identities (EBS admins, DBAs, service accts)	Privilege misuse for data export/exfil	Excess privilege; weak MFA/PAM; shared accounts	4	5	20 Critical	PAM + MFA for admins; least privilege; break-glass controls; rotate secrets/keys
Sensitive data stores (HR/finance/customer PII)	Mass theft for extortion / publication	Over-broad access; weak segmentation; weak DLP	4	5	20 Critical	Data classification; DLP; segmented access; encryption; query/export controls; monitoring for bulk access
Network segmentation & perimeter controls	Pivot from EBS to internal systems	Flat network; permissive east–west traffic	3	5	15 High	Zero Trust access paths; micro-segmentation; restrict DB/admin ports; egress controls
Logging/SIEM & detection engineering	Long dwell time / stealthy data theft	Missing app-aware telemetry and alerting	3	4	12 High	Centralise EBS/DB logs; alert on anomalous template creation, bulk exports, suspicious admin activity

Asset type	**Primary threat scenario (linked to the case)**	**Key vulnerability/weakness**	**L**	**I**	**Score**	**Targeted mitigation**
Patch & vulnerability management process	Repeat exposure to future enterprise zero-days	Incomplete asset inventory; slow emergency patching	4	4	16 Critical	Patch SLAs by severity; asset ownership; continuous scanning; emergency change process
Admin endpoints / jump hosts	Credential theft leading to privileged access	Weak hardening; local admin rights	3	4	12 High	Hardened jump hosts; EDR; block credential dumping; remove local admin; device posture checks
Backups & recovery systems	Secondary ransomware/extortion pressure	Untested restores; backup exposure to attackers	3	4	12 High	Immutable backups; offline copies; regular restore testing; separate backup credentials
Third parties (EBS support, hosting, integrators)	Supply-chain access or delayed patching	Unclear shared responsibilities; weak assurance	3	4	12 High	Contractual security clauses; patch responsibility matrix; vendor assurance reviews; audit rights

Table 5 Likelihood x Impact Template

Prioritised mitigation strategy

- **Top priority (Critical risks)**

1. **Close the initial access path** by applying Oracle's fix for CVE-2025-61882 and reducing exposure (remove direct internet access; enforce controlled access routes and filtering). Oracle and national guidance both emphasise urgent patching and compromise hunting due to likely exploitation.

2. **Assume compromise and eradicate persistence** by hunting for database-resident artefacts (including suspicious BI Publisher template activity) and validating integrity of EBS content repositories, as highlighted in Mandiant's guidance.

3. **Lock down privilege and stop bulk theft** through PAM/MFA, least privilege, strong separation of duties, and monitoring for abnormal export/query patterns because the campaign's value comes from rapid data exfiltration and extortion leverage.

4. **Harden governance and response readiness**: define emergency patch SLAs, owners for each EBS component, and executive extortion playbooks, so decision-making remains evidence-led under pressure.

- **Secondary priority (High risks)**

5. **Reduce blast radius** via segmentation and egress control to limit lateral movement and data staging.
6. **Improve detection** by forwarding EBS/DB audit signals into SIEM and creating detections tailored to this incident (template abuse, abnormal admin actions).
7. **Resilience**: immutable backups and tested recovery reduce the chance of extortion turning into prolonged outage.
8. **Supplier assurance** ensures patching, monitoring, and incident handling responsibilities are contractually clear and auditable.

Compliance linkage

This risk treatment approach directly supports **integrity and confidentiality** and **accountability** under UK GDPR by demonstrating a documented, prioritised control strategy for high-impact personal data processing, and it strengthens breach readiness for timely assessment/reporting obligations where applicable.

Chapter 3

Completing the Immersive Labs modules (Command Line Introduction, Moving Around, Linux File Permissions, Cyber Million: Cyber Safety, and Cyber Million: Staying Safe Online) and the Cisco Cyber Essentials labs strengthened both my technical foundations and my security mindset. The command line modules improved my confidence working in Linux environments, particularly navigating directories efficiently and using file and permission controls correctly. Learning how permissions map to real security outcomes made access control feel less "theory-based" and more like a practical safeguard that can prevent unauthorised reading, editing, or execution of sensitive files. This directly connects to the principles of least privilege and secure configuration that underpin secure system design.

The Cyber Million modules reinforced day-to-day cyber hygiene and helped me think about risk from a human perspective, including how social engineering, unsafe browsing, weak passwords, and poor device practices can undermine even well-designed technical controls. These lessons improved how I assess security risk: I now consider user behaviour as part of the attack surface and view awareness as a control that must be designed into processes, not assumed.

Finaly, these labs increased my ability to apply security best practices within this assignment especially around access control, safe configuration, and incident awareness and they highlighted the importance of combining technical safeguards with user-focused controls to reduce realistic threats in operational environments.

References

- European Data Protection Board (EDPB) (2020) *Guidelines 3/2019 on processing of personal data through video devices (Final version).* [online] Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
- Information Commissioner's Office (ICO) (n.d.) *Data protection by design and default.* [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-default/
- Information Commissioner's Office (ICO) (n.d.) *CCTV and video surveillance.* [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
- legislation.gov.uk (n.d.) *Regulation (EU) 2016/679, Article 25: Data protection by design and by default.* [online] Available at: https://www.legislation.gov.uk/eur/2016/679/article/25
- legislation.gov.uk (2018) *Data Protection Act 2018.* [online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents
- UK Government (GOV.UK) (n.d.) *Data protection and your business: Using CCTV.* [online] Available at: https://www.gov.uk/data-protection-your-business/using-cctv
- ISO/IEC 27001 as the assurance backbone use the ISMS to implement governance, risk assessment/treatment, supplier assurance, incident management and continual improvement over the full system scope. [online] Available at: https://www.iso.org/standard/27001
- NIST CSF 2.0 as the operational security roadmap organise day-to-day security outcomes and maturity improvements across Govern Recover, ensuring monitoring and resilience are continuous rather than one-off. [online] Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- Cyber Essentials as the baseline "anti-common-attacks" control set ensure the most common internet-based weaknesses are systematically addressed across endpoints and infrastructure supporting CCTV/FRT/tracing. [online] Available at: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf
- Google Threat Intelligence Group (GTIG) & Mandiant (2025) *Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign.* Google Cloud Blog, 9 October. [online] Available at: https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation
- NHS England (2025) *Oracle Releases Security Advisory for E-Business Suite (CC-4705).* NHS England Digital, 6 October. [online] Available at: https://digital.nhs.uk/cyber-alerts/2025/cc-4705
- National Vulnerability Database (NVD) (2025) *CVE-2025-61882 Detail.* National Institute of Standards and Technology. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2025-61882
- Oracle (2025) *Oracle Security Alert Advisory – CVE-2025-61882.* Oracle. [online] Available at: https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
- Oracle (2025) *Critical Patch Update Advisory – October 2025.* Oracle. [online] Available at: https://www.oracle.com/security-alerts/cpuoct2025.html