* 1. **Security controls notes**

**Categories**

Technical –

Managerial –

Operational –

Physical –

**Control types**

Preventive –

Detective –

Corrective –

Directive –

Deterrent –

Compensating –

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**1.2 Security concepts notes**

**CIA** –

Confidentiality –

Integrity –

Availability –

**Non-repudiation** –

**Cybersecurity Framework** –

Identify –

Protect –

Detect –

Respond –

Recover –

**Why use a framework?** –

**Gap analysis** –

**Access control** –

Subjects –

Objects –

**IAM** –

Identification –

Authentication –

Authorization –

Accounting –

**Zero Trust** –

**Control plane** –

The policy decision point is comprised of two subsystems:

Policy Engine –

Policy Administrator –

Adaptive identity –

Threat scope reduction –

Policy-driven access control –

**Data plane** –

Subject / System –

Policy Enforcement Point –

Implicit trust zones –

**Physical security** –

Bollards –

Access control vestibule –

Fencing –

Video surveillance –

Security guard –

Access Badge –

Lighting –

Sensors –

Infrared Sensors –

Pressure Sensors –

Microwave Sensors –

Ultrasonic Sensors –

**Deception and Disruption technology** –

Honeypot –

Honeynet –

Honeyfile –

Honeytoken –

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**1.3 Change management**

**Business processes impacting security operation** –

Ownership –

Stakeholders –

**Change Management Concepts:**

Impact analysis –

Test results –

Backout plan –

Maintenance window –

Standard operating procedure (SOP) –

**Technical implications** –

Allow lists/deny list –

Restricted activities –

Downtime –

Service restart –

Application restart –

Legacy applications –

Dependencies –

**Version control** –

**Documentation**

Upgrading diagrams –

Upgrading policies/procedures –

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**1.4 Cryptographic solutions**

**Public key infrastructure** –

Public key –

Private key –

Key escrow –

**Encryption** –

Levels –

Full disk encryption (FDE) –

Partition –

File encryption –

Volume encryption –

Database-level encryption –

Record-level encryption –

Asymmetric –

Symmetric –

Transport / communication –

Wi-fi Protected Access (WPA) –

Internet Protocol Security (IPsec) –

Transport Layer Security (TLS) –

Key exchange –

Algorithms –

Key length –

**Tools** –

There are two main ways of implementing cryptoprocessor hardware:

Trusted platform module (TPM) –

Hardware security module (HSM) –

Secure enclave –

Key management system –

**Obfuscation** –

Steganography –

Tokenization –

Data masking –

**Hashing** –

There are two popular implementations of hash algorithms:

Secure Hash Algorithm **(SHA)** –

Message Digest Algorithm #5 **(MD5)** –

**Salting** –

**Brute force attack** –

**Dictionary attack** –

**Digital signatures** –

**Key stretching** –

**Blockchain** –

**Open public ledger** –

**Certificates** –

Certificate authorities –

Certificate revocation lists (CRL) –

Revoked –

Suspended –

Online certificate status protocol (OCSP) –

Self-signed –

Third-party –

Root of trust –

Certificate signing request generation (CSR) –

Wildcard –