**📘 Summary: 01 Introduction and High Level Overview**

**1. What is Security Operations Management (SecOps)?**

* **Goal:** Manage key security concerns effectively across:
  + **What:** Network, Infrastructure, Data, Users
  + **Where:** At rest, in transit, in use
  + **Who manages:** Users, Admins, Business, Security professionals

**2. Security Operations Management Approaches & Tools**

* **Actionable processes**
* **Security Architecture**
* **Operational Models**: TOGAF, NIST, ISO, MITRE, CSA, COBIT, ITIL
* **Blueprints:**
  + Master Plan
  + Architecture
  + Action Guidance

**3. 3 Lines of Defence Model (3LD)**

1. **First Line** – Operation of security controls
2. **Second Line** – Compliance and risk assessment
3. **Third Line** – Independent audit

**4. Security Operations Flow: From Requirements to Architecture**

* **Inputs:**
  + Business, Legal, Regulatory, Organisational Requirements
* **Outputs:**
  + Network, Infrastructure, Data, Application, User Security
  + Cloud (Public/Private/Hybrid), On-Premises, Off-Site

**5. Security Operation Reference Architecture**

* Covers:
  + Governance, Strategy, Risk
  + Architecture & Policies
  + Threat & Vulnerability Management
  + Monitoring & Incident Management
  + IAM
  + Physical Security
  + Security Awareness and Training
  + Continuous Improvement

**6. Course Focus**

* Understand full scope and boundaries of SecOps
* Understand **people, process, technology** components
* Apply foundational cybersecurity knowledge in operational context

**7. Course Outline**

* **12 Online Lectures**
  + Wednesdays, attendance mandatory
* **4 Labs** (Saturdays, 9–3:30), submissions due by next lecture
* **Final Exam**
  + Similar to “Security Fundamentals” exam

**8. Tools & Platforms Required**

* Moodle
* Microsoft Office (CityColleges Account)
* CompTIA Labs Platform

**9. Recap of Security Fundamentals**

**Topics reviewed:**

* Security Concerns, Stakeholders, Control Categories
* Frameworks & Standards (NIST, ISO)
* Threat Actors, Vulnerabilities, Tooling
* Cryptography, IAM, Network & Host Security
* Application Security, Cloud Security
* Incident Response, Digital Forensics
* Risk Management, BIA, BCP, DR
* Physical Security & Redundancy

**10. Security Operations Objectives**

* Deliver comprehensive security services
* Define and follow structured processes
* Use well-configured technology
* Employ competent staff

**11. Summary of Key Components**

* **Foundational Elements:**
  + Governance
  + Architecture
  + Strategy
  + Operations
* **Supporting Functions:**
  + Identity & Access Management
  + Risk & Compliance
  + Training & Awareness
  + Incident Response