# Exam Content Outline

1. **Business and Security Environment (ID)  25%**
   - **1A** Business Environment
     - 1A1 Digital Infrastructure
     - 1A2 Enterprise Architecture
     - 1A3 Data and Digital Communication
   - **1B** Security Environment
     - 1B1 Network
     - 1B2 Operating Systems
     - 1B3 Applications
     - 1B4 Virtualization and Cloud

2. **Operational Security Readiness (PR)  25%**
   - **2A** Protection
     - 2A1 Digital and Data Assets
     - 2A2 Ports and Protocols
     - 2A3 Protection Technologies
     - 2A4 Identity and Access Management
     - 2A5 Configuration Management
   - **2B** Preparedness
     - 2B1 Threat Modeling
     - 2B2 Contingency Planning
     - 2B3 Security Procedures

3. **Threat Detection and Evaluation (DE)  25%**
   - **3A** Monitoring
     - 3A1 Vulnerability Management
     - 3A2 Security Logs and Alerts
     - 3A3 Monitoring Tools and Appliances
     - 3A4 Use Cases
     - 3A5 Penetration Testing
   - **3B** Analysis
     - 3B1 Network Traffic Analysis
     - 3B2 Packet Capture and Analysis
     - 3B3 Data Analysis
     - 3B4 Research and Correlation

4. **Incident Response and Recovery (RS&RC)  25%**
   - **4A** Incident Handling
     - 4A1 Notifications and Escalation
     - 4A2 Digital Forensics
   - **4B** Mitigation
     - 4B1 Containment
     - 4B2 Attack Countermeasures
     - 4B3 Corrective Actions
   - **4C** Restoration
     - 4C1 Security Functions Validation
     - 4C2 Incident Analysis and Reporting
     - 4C3 Lessons Learned and Process Improvement