Suggested Topics for Review

1. **Strategy, Governance & Compliance**
   - 1.1. Readiness for Emerging Cyber Threats
   - 1.2. Secure by Design Principles
   - 1.3. Risk Management, Governance and Compliance
   - 1.4. Regulatory Compliance and Industry Standards
   - 1.5. Cyber Resilience and Business Continuity
2. **OT Architecture & Infrastructure Security**
   - 2.1. Zero Trust Architecture for OT Environments
   - 2.2. IT/OT Segmentation and Secure Network Architecture
   - 2.3. Network and Communications Security
   - 2.4. Secure Remote Access
   - 2.5. Security of Industrial Communication Protocols
   - 2.6. Cloud, Edge and Industrial IoT Security
   - 2.7. AI Infrastructure and Systems Security
3. **Security Operations & Incident Management**
   - 3.1. Threat Monitoring, Detection and Security Event Visibility
   - 3.2. Vulnerability Management
   - 3.3. Cyber Threat Intelligence and Proactive Defense
   - 3.4. Incident Response and Recovery
4. **Identity, Access & Asset Protection**
   - 4.1. Identity and Access Management
   - 4.2. Server, Workstation and Endpoint Security
   - 4.3. Asset Security and Asset Inventory Management
   - 4.4. Data Protection and Information Security
   - 4.5. Cyber-Physical Systems Security
5. **Supply Chain & Third-Party Security**
   - 5.1. Supplier and Supply Chain Security Management
   - 5.2. Third-Party Risk Management
6. **Application & Software Security**
   - 6.1. Application and Software Security
   - 6.2. Secure Software Development Lifecycle
   - 6.3. Software Supply Chain Security
7. **Awareness & Stakeholders**
   - 7.1. System security Training
   - 7.2. Owner, Integrator, Supplier, Service provider - Cybersecurity Engagement