

Foundations, Structures and Controls of Cybersecurity

Student Guide



Dr Diarmuid Ó Briain
Version: 1.0

Copyright © 2026 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



1 Abstract

This module provides a comprehensive, hands-on exploration of cybersecurity across three critical dimensions: engineering infrastructure, strategic governance, and crisis operations. Utilising a Team-Based Learning (TBL) model, learners transition from foundational knowledge to active technical execution across three cohesive themes.

- **Theme 1 (OT Infrastructure & Foundational Security)** establishes the technical baseline, contrasting traditional IT with specialised Operational Technology (OT) environments. Students master the architectural layers of the Purdue Model, industrial hardware, and the essential physical and logical access controls required to safeguard critical infrastructure. Theme Capstone: Designing a comprehensive physical and digital access policy for a critical manufacturing plant.
- **Theme 2 (Governance, Risk, and Compliance)** shifts focus from technical perimeters to corporate strategy. Students examine how organizations align security operations with global frameworks (NIST CSF, ISO-27001, ITIL, COBIT), quantify threat landscapes, and navigate legal, compliance, and regulatory obligations. Theme Capstone: Conducting an executive-level corporate risk assessment and compliance audit.
- **Theme 3 (Offensive Security & Incident Response)** moves into tactical, adversarial operations. Learners explore the mechanics of penetration testing to discover systemic vulnerabilities before learning the defensive strategies required to handle the worst-case scenario. Theme Capstone: A real-time, high-stakes tabletop simulation to triage and contain an active, evolving data breach.

2 Module Aim

Provide learners with the ability to combine Industrial Automation and Control Systems (IACS) systems and protocols with Cybersecurity frameworks and tools in order to prepare the model for incident response plans to counteract the cyber attacks.

3 Learning Outcomes

On successful completion of this module the learner should be able to:

- Visualise Operational Technology as they are employed in manufacturing, distribution and critical infrastructure.
- Construct a business case for Security of Operational Technology.
- Consider Cyber Security Architectures applicable to the security of Operational Technology.
- Categorise physical and digital access controls as they apply to the security of Operational Technology.
- Appraise risk management, risk assessment and the execution of risk management tasks in the context of Operational Technology security.

4 Module Operation

To gain maximum benefit from this module and to ensure you gain practical, real-world skills, this module implements a structured Team-Based Learning (TBL) model.

The module is divided into three major core themes. Each theme follows an identical stepped lifecycle designed to move you from foundational knowledge to problem solving.

Here is exactly how you will navigate each of the three theme blocks:

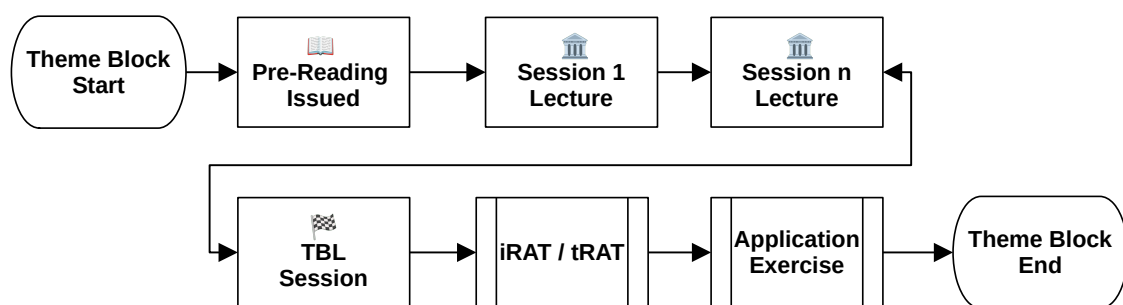


Figure 1: Navigating each theme block

4.1 Breakdown of the Steps

Pre-Reading & Self-Study

At the start of each theme, you will receive a targeted Pre-Reading Packet. This packet contains essential vocabulary, industry definitions, and context. By covering this material as independent learning it ensures everyone in the classroom is using the same technical language.

Interactive Live Sessions

Because the basic terms are already completed in the Pre-Reading and Self-Study the live lecture sessions will dive straight into deeper more complex concepts.

The TBL Session (The Climax)

The final session of the block is where everything comes together. It consists of two parts:

1. **Readiness Assurance (iRAT/tRAT):** A short, competitive quiz taken first individually, then immediately again within a designated team. This tests your grasp of the Pre-Reading material and the live sessions.
2. **Team Application Exercise:** Each team will be handed a complex, real-world scenario or incident. Using the collective knowledge built over the block, each team must diagnose the scenario and propose an engineered solution.

5 Table of Contents

Theme 1: OT Infrastructure & Foundational Security

Understanding specialised environments (Operational Technology) and the baseline perimeter defences that protect them.

The theme establishes what is being protected (OT vs. IT environments) and the most fundamental layers of security. A great TBL application exercise here would be.

- **Pre-Reading:** Foundations, History & Taxonomy
- **Topic 1:** Industrial Environments & the Purdue Architecture
- **Topic 2:** Hardening OT Components & Physical Boundaries
- **Topic 3:** Layered Logical Access Control & Core Protocols
- **TBL 1:** Design a secure entry and access policy for a critical manufacturing facility

Theme 2: Governance, Risk, and Compliance (GRC)

The strategic, legal, and programmatic frameworks used to manage organisational risk and satisfy regulators. This moves the module from technical controls to understanding executive strategy. How to assess threat landscapes and align security with international standards.

- **Pre-Reading:** Strategic GRC Foundations & Taxonomy
- **Topic 4:** Enterprise Risk Management Frameworks & Threat Quantification
- **Topic 5:** Strategic Governance & Operational Security Frameworks
- **Topic 6:** ISMS Architecture, Regulatory Audits & Forensic Readiness
- **TBL 2:** Auditing a company against a framework and conducting a high-level risk assessment.

Theme 3: Offensive Security & Incident Response

Proactively testing defences and executing reactive strategies when a security breach occurs.

- **Pre-Reading:** Threat Fundamentals & Environment Setup
- **Topic 7:** Proactive Defence & Offensive Reconnaissance
- **Topic 8:** Incident Response & Breach Management (Immersive Simulation)
- **TBL 3:** The Recce-to-Response Crisis.

6 Table of Abbreviations

2FA	Two-Factor Authentication
AAA	Authentication, Authorisation, Accounting
ACK	ACKnowledge
ACL	Access Control List
ACS	Annual Cost of Safeguard
ACS	Automation and Control Systems
AI	Artificial Intelligence
AIC	Availability, Integrity, Confidentiality
ALE	Annualised Loss Expectancy
APO	Align, Plan and Organise
ARO	Annualised Rate of Occurrence
ARP	Address Resolution Protocol
AS	Authentication Server
ATO	Authorisation to Operate
ATU	Authorisation to Use
AV	Asset Value
BAI	Build, Acquire and Implement
BCP	Business Continuity Plan
BMS	Building Management Systems
CA	Companies Act
CAP	Corrective Action Plan
CBA	Cost Benefit Analysis
CBI	Central Bureau of Investigation
CC	Common Criteria
CC	Common Criteria
CCPA	California Consumer Privacy Act
CCRA	Common Criteria Recognition Arrangement
CCTV	Close Circuit TeleVision
CDN	Content Deliver Network
CEO	Chief Executive Officer
CER	Crossover Error Rate
CERT-In	Indian Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, Availability
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMA	Computer Misuse Act
CMM	Capability Maturity Model
CNI	Critical National Infrastructure
COBIT	Control Objectives for Information and Related Technology
COBOL	COmmon Business-Oriented Language
COCOM	Coordinating Committee for Multilateral Export Controls
CoE	Council of Europe
COO	Chief Operating Officer
COPPA	Children's Online Privacy Protection Act
COSO	Committee of Sponsoring Organisations
CP	Control Point
CP	Controls points
CRA	EU Cyber Resilliance Act
CRM	Cybersecurity Risk Management

CSF	Cybersecurity Framework
CSO	Chief Security Officer
DAC	Discretionary Access Controls
DCS	Distributed Control Systems
DE	Detect
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DiD	Defence-in-Depth
DMZ	De-Militarised Zone
DNP3	Distributed Network Protocol version 3
DORA	Digital Operational Resilience Act
DoS	Denial of Service
DPA	Data Protection Authority
DPDP	Indian Digital Personal Data Protection Act
DSP	Digital Service Providers
DSS	Data Security Standard
DSS	Deliver, Service and Support
DVR	Digital Video Recorders
EAR	Export Administration Regulations
ECO	Export Control Order
EDM	Evaluate, Direct and Monitor
EF	Exposure Factor
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
ESB	Electricity Supply Board
EUCC	EU Cybersecurity Certification Scheme on Common Criteria
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FCPA	US Foreign Corrupt Practices Act
FCRA	air Credit Reporting Act
FCS	Fire Control Systems
FISMA	Federal Information Security Modernization Act
FRR	False Rejection Rate
GCHQ	UK's Government Communications Headquarters
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GSLB	Global Server Load Balancing
GV	Govern
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HLS	High-Level Structure
HMI	Human Machine Interfaces
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilating, and Air Conditioning
IACS	Industrial, Automation and Control Systems
ICIF	Internal Control - Integrated Framework
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ICT	Information Communications Technology
ID	IDentification
ID	Identify
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device

IETF	Internet Engineering Task Force
IOT	Internet of Things
IP	Internet Protocol
IPC	Indian Penal Code 1860
IPC	Industrial PC
IPS	Intrusion Prevention System
IRP	Incident Response Plan
IRT	Isochronous Real-Time
IS	Information Systems
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Information Security Policy
ISP	Internet Service Provider
IT	Information Technology
ITADA	Identity Theft and Assumption Deterrence Act
ITAM	IT Asset Management
ITIL	IT Infrastructure Library
ITSM	IT Service Management
KDC	Key Distribution Centre
LBAC	Lattice-based Access Control
Ma-NC	Major Non Conformity
MAC	Mandatory Access Control
MEA	Monitor, Evaluate and Assess
MeitY	Ministry of Electronics and Information Technology
MERCOSUR	MERCado COMún del SUR Southern Common Market
MFA	Multi-Factor Authentication
Mi-NC	Minor Non Conformity
MitM	Man-in-the-Middle
MLS	Multi-Level Secure
MO	Modus Operandi
MOM	Opportunity and Motives
MRT	Management Review Team
NAFTA	North American Free Trade Agreement
NAT	Network Address Translation
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreements
NIDS	Network-based IDS
NIDS	Network Intrusion Detection Systems
NIS2	Network Information Systems version 2
NIST	National Institute of Standards and Technology
NMAP	Network Mapper
nonce	Number used ONCE
NPSA	National Protective Security Authority
NSE	NMAP Scripting Engine
NT	Network Technician
NTP	Network Time Protocol
NVR	Network Video Recorders
OBP	Online Browsing Platform
OES	Operators of Essential Services
OFI	Opportunity for Improvement
OGC	Office of Government Commerce
OS	Operating Systems

OT	Operational Technology
OTP	One Time Password
OTSec	OT Security
PACS	Physical Access Control Systems
PC	Personal Computer
PCI	Payment Card Industry
PECR	Privacy and Electronic Communications
PICERL	Preparation-Identification-Containment-Eradication-Recovery-Lessons Learned
PID	Proportional-Integral-Derivative
PIDS	Protocol-based Intrusion Detection System
PII	Personally Identifiable Information
PIN	Personal Identification Number
PING	Packet InterNet Groper
PLC	Programmable Logic Controller
POAM	Plan of Action and Milestones
POCA	Prevention of Corruption Act
PPE	Personal Protective Equipment
PR	Protect
Profinet	Process Field Network
RADIUS	Remote Access Dial-in User Service
RBAC	Role-based Access Control
RC	Recover
RDM	Remote Diagnostics & Maintenance
RMF	Risk Management Framework
RMP	Risk Management Plan
RS	Respond
RTOS	Real Time Operating System
RTU	Remote Terminal Units
SAML	Security Assertion Markup Language
SBU	Sensitive but Unclassified
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Control Transmission Protocol
SDLC	Secure Development Lifecycle
SEC	Securities and Exchange Commission
SFO	Serious Fraud Office
SIS	Safety Instrumented Systems
SLA	Service Level Agreements
SLE	Single Loss Expectancy
SMARTER	Specific-Measurable-Achievable-Relevant-Time-bound-Evaluate-Re-evaluate
SME	Subject Matter Expert
SMS	Short Messaging Service
SMT	Senior Management Team
SoA	Statement of Applicability
SoD	Separation of Duties
SoP	Separation of Powers
SP	Special Publication
SRT	Soft-Real Time
SS	Service Server
SSH	Secure Shell
SSO	Single Sign On
SYN	SYNchronise
TACACS	Terminal Access Controller Access Control System

TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TGS	Ticket Granting Server
TOR	The Onion Router
TSN	Time-Sensitive Networking
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VCDPA	Virginia Consumer Data Protection Act
WTO	World Trade Organisation

7 Supplementary Book Resources

Pascal Ackerman 2017, Industrial Cybersecurity, Packt Publishing Ltd [ISBN: 9781788395984]

Eric D. Knapp, Joel Langill 2014, Industrial Network Security, Syngress Press [ISBN: 0124201148]

Edward J. M. Colbert, Alexander Kott 2018, Cyber-security of SCADA and Other Industrial Control Systems, 1 Ed., 16, Springer
[ISBN: 3319812033]

8 Recommended Article/Paper Resources

US National Institute of Standards and Technology (NIST) 2024, The NIST Cybersecurity Framework (CSF) 2.0.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

US National Institute of Standards and Technology (NIST) 2015, Guide to Operational Technology (OT) Security Revision 3, Initial Public Draft, NIST SP 800-82r3 ipd.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf>

US National Institute of Standards and Technology (NIST) 2020, Security and Privacy Controls for Information Systems and Organizations to OT', NIST SP 800-53 Rev. 5.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf>