Operational Technology Cybersecurity for Energy

GExperts Learning Academy | PC-X19 | PC | 12-18 weeks

Course overview

12-18 weeks PC programme focused on Operational Technology Cybersecurity for Energy, using energy-sector cases and applied decisions.

Designed for: Experienced professionals

Learning outcomes

- Explain core principles and terminology for Operational Technology Cybersecurity for Energy.
- Interpret an applied case using evidence and stated assumptions.
- Identify risks, safeguards, role boundaries and escalation points.
- Prepare a clear recommendation for a multidisciplinary audience.

Course guide

Work through each module objective, lesson and teaching note, complete the applied activity and assessment, then use the separate Academy practice page for practice questions and answer feedback.

Separate practice questions:
https://www.globalexpertsconsultoria.com/training/academy/courses/questions/?course=PC-X19

Academic and certification status

Draft learning resource for study and review. It does not confer accreditation, external certification, a regulated qualification, professional licence, safety-critical competence or site authorisation. Confirm approvals, current laws, standards, approved procedures and awarding-body requirements before delivery.

Module 1: OT and ICS cybersecurity awareness

Learning objectives

- Explain ot and ics cybersecurity awareness, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of OT and ICS cybersecurity awareness
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Operational technology controls physical processes, so availability, safety and predictable operation are central. Explain assets, zones, connections, remote access and dependencies conceptually. Security controls must be coordinated with operational and safety requirements.

Decision logic. Use a tabletop risk assessment on fictional architecture. Inventory, controlled access, segmentation, backup and recovery are discussion topics, not permission for live changes or scanning. Approved change and incident procedures govern actual systems.

Worked example. An unrecorded remote-support connection bypasses the fictional architecture's reviewed access path.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Identify risk and propose review questions without touching any real network.

Model answer guide. Request asset ownership, approved access route, monitoring, recovery and safety coordination.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Identify risk and propose review questions without touching any real network.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 2: Information security management systems

Learning objectives

- Explain information security management systems, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Information security management systems
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. An ISMS establishes governance for protecting information through risk management, responsibilities, controls and continual improvement. Define scope, interested parties and information assets before selecting controls. This is original awareness content informed by the supplied implementation proposal.

Decision logic. Connect risk treatment, documented decisions, monitoring, audit and corrective action. Obtain licensed standards for formal implementation and verify external certification requirements with the relevant body. This course does not award PECB or ISO certification and reproduces no official examination.

Worked example. A fictional academy protects student records through defined access, retention and incident responsibilities.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Draft an ISMS scope, three risks and a treatment review plan.

Model answer guide. Require risk owners, justified treatments, evidence, review and escalation; distinguish organisational certification from personal credentials.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Draft an ISMS scope, three risks and a treatment review plan.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 3: Operational Technology Cybersecurity for Energy: Systems and In

Learning objectives

- Explain operational technology cybersecurity for energy: systems and interfaces, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Operational Technology Cybersecurity for Energy: Systems and Interfaces
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Operational Technology Cybersecurity for Energy: Systems and Interfaces describes a practical part of Operational Technology Cybersecurity for Energy. Learners connect the principles to asset performance, people, operational risk, project value and local context.

Decision logic. Review the objective, evidence, limits, interfaces and applicable controls for operational technology cybersecurity for energy: systems and interfaces. Decisions require current information, role-appropriate authority, competent review and documented assumptions.

Worked example. Use an applied Namibia-relevant case in which a team plans operational technology cybersecurity for energy: systems and interfaces while balancing safety, integrity, schedule, cost, environmental protection and local capability.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Prepare a decision brief for operational technology cybersecurity for energy: systems and interfaces: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Model answer guide. A sound response defines scope; uses current, traceable evidence; applies approved requirements and controls; records assumptions; assigns competent owners; checks interfaces; and communicates a measurable decision with an escalation path.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Prepare a decision brief for operational technology cybersecurity for energy: systems and interfaces: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 4: Umbilicals and subsea control systems

Learning objectives

- Explain umbilicals and subsea control systems, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Umbilicals and subsea control systems
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Umbilicals transmit combinations of power, communications, hydraulic service and chemicals. Subsea controls command and monitor equipment. Use a signal-and-energy diagram to separate commands, feedback and physical actuation.

Decision logic. Control philosophy must address loss of power, communications and hydraulic supply, plus the intended safe response. Check compatibility and redundancy across surface and subsea equipment. A command acknowledgement does not necessarily prove final valve position.

Worked example. A control command is received, but independent position feedback disagrees. Investigate rather than assume successful actuation.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Trace one command path and identify three failure points and their indication.

Model answer guide. Include surface control, communication, power or hydraulic supply and feedback; distinguish received command from achieved state.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Trace one command path and identify three failure points and their indication.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 5: Incident investigation and learning

Learning objectives

- Explain incident investigation and learning, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Incident investigation and learning
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. An investigation establishes what happened, why controls failed and how recurrence can be prevented. Preserve evidence, protect people and separate verified facts from assumptions. Near misses can reveal major weaknesses without actual harm.

Decision logic. Use a timeline and causal analysis to explore technical, human and organisational contributors. Avoid premature blame and unsupported conclusions. Actions should address causes, have accountable owners and be checked for effectiveness. Reporting follows applicable site and legal requirements.

Worked example. A dropped tool caused no injury, but exclusion-zone and securing controls were ineffective.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Analyse a fictional near miss and propose three causal actions.

Model answer guide. Include physical prevention, work-system improvements and verification, rather than retraining alone.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Analyse a fictional near miss and propose three causal actions.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 6: SCADA DCS and integrated control systems

Learning objectives

- Explain scada dcs and integrated control systems, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of SCADA DCS and integrated control systems
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Control systems acquire signals, execute logic and support operator actions. SCADA, DCS and integrated control architectures differ by context; safety functions require appropriate separation and assurance. Explain sensor, controller, final element and human interface.

Decision logic. Alarm and control design must match process needs and human capability. More alarms do not necessarily improve safety. Changes to logic require controlled review, testing and approval. This course uses simulation only and provides no live-system modification instructions.

Worked example. An alarm floods the operator screen during a simulated upset, obscuring the initiating condition.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Map a control loop and evaluate an alarm list for prioritisation questions.

Model answer guide. Identify measurement, logic, final element and feedback, with rationalised alarms and change control.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Map a control loop and evaluate an alarm list for prioritisation questions.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 7: Operational Technology Cybersecurity for Energy: Applied Case

Learning objectives

- Explain operational technology cybersecurity for energy: applied case, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Operational Technology Cybersecurity for Energy: Applied Case
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Operational Technology Cybersecurity for Energy: Applied Case describes a practical part of Operational Technology Cybersecurity for Energy. Learners connect the principles to asset performance, people, operational risk, project value and local context.

Decision logic. Review the objective, evidence, limits, interfaces and applicable controls for operational technology cybersecurity for energy: applied case. Decisions require current information, role-appropriate authority, competent review and documented assumptions.

Worked example. Use an applied Namibia-relevant case in which a team plans operational technology cybersecurity for energy: applied case while balancing safety, integrity, schedule, cost, environmental protection and local capability.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Prepare a decision brief for operational technology cybersecurity for energy: applied case: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Model answer guide. A sound response defines scope; uses current, traceable evidence; applies approved requirements and controls; records assumptions; assigns competent owners; checks interfaces; and communicates a measurable decision with an escalation path.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Prepare a decision brief for operational technology cybersecurity for energy: applied case: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 8: Petroleum policy and institutional governance

Learning objectives

- Explain petroleum policy and institutional governance, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Petroleum policy and institutional governance
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Policy sets objectives, institutions assign authority, and governance creates accountability for decisions and resources. Explain government, regulator and state enterprise roles conceptually without asserting an unverified current Namibian structure.

Decision logic. Separate commercial participation from regulatory judgement and manage conflicts transparently. Define decision rights, disclosure, assurance and challenge. A strong governance design includes implementation capacity and an audit trail, not just an organisation chart.

Worked example. A fictional institution both promotes investment and evaluates its own project compliance, creating a conflict to manage.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Draft a responsibility matrix and conflict-management controls.

Model answer guide. Identify segregated decisions, independent review, declarations and public accountability where applicable.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Draft a responsibility matrix and conflict-management controls.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 9: Operational Technology Cybersecurity for Energy: Knowledge Che

Learning objectives

- Explain operational technology cybersecurity for energy: knowledge check, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Operational Technology Cybersecurity for Energy: Knowledge Check
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Operational Technology Cybersecurity for Energy: Knowledge Check describes a practical part of Operational Technology Cybersecurity for Energy. Learners connect the principles to asset performance, people, operational risk, project value and local context.

Decision logic. Review the objective, evidence, limits, interfaces and applicable controls for operational technology cybersecurity for energy: knowledge check. Decisions require current information, role-appropriate authority, competent review and documented assumptions.

Worked example. Use an applied Namibia-relevant case in which a team plans operational technology cybersecurity for energy: knowledge check while balancing safety, integrity, schedule, cost, environmental protection and local capability.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Prepare a decision brief for operational technology cybersecurity for energy: knowledge check: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Model answer guide. A sound response defines scope; uses current, traceable evidence; applies approved requirements and controls; records assumptions; assigns competent owners; checks interfaces; and communicates a measurable decision with an escalation path.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Prepare a decision brief for operational technology cybersecurity for energy: knowledge check: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Module 10: Operational Technology Cybersecurity for Energy: Competence R

Learning objectives

- Explain operational technology cybersecurity for energy: competence review, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Operational Technology Cybersecurity for Energy: Competence Review
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Operational Technology Cybersecurity for Energy

Detailed teaching notes

Teaching notes

Core explanation. Operational Technology Cybersecurity for Energy: Competence Review describes a practical part of Operational Technology Cybersecurity for Energy. Learners connect the principles to asset performance, people, operational risk, project value and local context.

Decision logic. Review the objective, evidence, limits, interfaces and applicable controls for operational technology cybersecurity for energy: competence review. Decisions require current information, role-appropriate authority, competent review and documented assumptions.

Worked example. Use an applied Namibia-relevant case in which a team plans operational technology cybersecurity for energy: competence review while balancing safety, integrity, schedule, cost, environmental protection and local capability.

Facilitator prompts. Ask learners to distinguish verified facts from assumptions, identify who has decision authority, name stop-work triggers and state what evidence could change their recommendation. Compare technical, HSE, commercial and community perspectives.

Activity. Prepare a decision brief for operational technology cybersecurity for energy: competence review: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Model answer guide. A sound response defines scope; uses current, traceable evidence; applies approved requirements and controls; records assumptions; assigns competent owners; checks interfaces; and communicates a measurable decision with an escalation path.

Assessment evidence. Score accuracy (30%), use of evidence (20%), safeguards (20%), analysis (20%) and communication (10%).

Applied activity

Prepare a decision brief for operational technology cybersecurity for energy: competence review: scope, evidence, assumptions, hazards, safeguards, owner, decision gate and escalation trigger.

Assessment

Formative: 10-question practice quiz with answer feedback

Summative: Applied decision brief or practical case assessed against the rubric; proposed pass mark 70%, subject to academic approval.

Practice

Use the separate Academy practice questions and answer key page for this module.

Facilitator close-out and resources

Facilitator close-out

Record attendance, assessment evidence, learner support needs, incidents and improvement actions according to approved provider processes. Do not sign learners off for regulated or safety-critical work without the authorised assessment and certification route.

Resources and references

- Supplied GExperts/IUM reference materials; verify reuse rights and currentness.
- Current applicable Namibian legislation, standards and approved site procedures supplied by the provider.
- Case worksheet and instructor slides must be produced and reviewed before course release.