Digital Oilfield, Automation and OT Cybersecurity Awareness

GExperts Learning Academy | SC-017 | SC | 1 days

Course overview

1 days SC programme focused on Digital Oilfield, Automation and OT Cybersecurity Awareness, using energy-sector cases and applied decisions.

Designed for: Learners appropriate to the stated programme level

Learning outcomes

- Explain core principles and terminology for Digital Oilfield, Automation and OT Cybersecurity Awareness.
- 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=SC-017

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: Industrial instrumentation

Learning objectives

- Explain industrial instrumentation, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Industrial instrumentation
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Sensors and transmitters convert process conditions into signals. Teach range, span, accuracy, calibration and measurement uncertainty. Pressure, temperature, flow and level measurements use different principles and installation constraints.

Decision logic. Trace a measurement from process interface through signal conversion to display. Incorrect range or units can mislead control and operations. An apparently stable value may be frozen or invalid. Actual instrument work follows authorised isolation and manufacturer procedures.

Worked example. A 4-20 mA signal represents 0-100 units; 12 mA corresponds to 50 units under a linear mapping.

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. Calculate the indicated value at 8 mA and identify assumptions.

Model answer guide. Twenty-five units with linear mapping and a valid signal; check range and status.

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

Applied activity

Calculate the indicated value at 8 mA and identify assumptions.

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: Industrial data architecture and governance

Learning objectives

- Explain industrial data architecture and governance, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Industrial data architecture and governance
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Industrial data flows from sensors through historians and integration platforms to analysis and decisions. Define asset identity, units, timestamps, quality status and ownership. A large dataset is not necessarily fit for purpose.

Decision logic. Check time synchronisation, missing values, calibration changes and access permissions before analysis. Keep provenance and revision history. Avoid transferring confidential operational data into exercises; all datasets in this package are fictional.

Worked example. A trend combines pressure in bar and kilopascals under one label, producing a false step change.

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. Create a data dictionary and quality checks for a fictional dataset.

Model answer guide. Define units, time basis, validity flags, owner and transformations; resolve inconsistent units before interpretation.

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

Applied activity

Create a data dictionary and quality checks for a fictional dataset.

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: 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: Digital Oilfield, Automation and OT Cybersecurity Awareness

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 4: 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: Digital Oilfield, Automation and OT Cybersecurity Awareness

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 5: Digital Oilfield, Automation and OT Cybersecurity Awareness: Wor

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: work planning, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Work Planning
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Work Planning describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: work planning. 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 digital oilfield, automation and ot cybersecurity awareness: work planning 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 digital oilfield, automation and ot cybersecurity awareness: work planning: 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 digital oilfield, automation and ot cybersecurity awareness: work planning: 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 6: Digital Oilfield, Automation and OT Cybersecurity Awareness: Data

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: data and performance, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Data and Performance
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Data and Performance describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: data and performance. 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 digital oilfield, automation and ot cybersecurity awareness: data and performance 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 digital oilfield, automation and ot cybersecurity awareness: data and performance: 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 digital oilfield, automation and ot cybersecurity awareness: data and performance: 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 7: Digital Oilfield, Automation and OT Cybersecurity Awareness: App

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: applied case, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Applied Case
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Applied Case describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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: Digital Oilfield, Automation and OT Cybersecurity Awareness: Con

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: communication and escalation, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Communication and Escalation
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Communication and Escalation describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: communication and escalation. 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 digital oilfield, automation and ot cybersecurity awareness: communication and escalation 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 digital oilfield, automation and ot cybersecurity awareness: communication and escalation: 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 digital oilfield, automation and ot cybersecurity awareness: communication and escalation: 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 9: Digital Oilfield, Automation and OT Cybersecurity Awareness: Kno

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: knowledge check, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Knowledge Check
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Knowledge Check describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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: Digital Oilfield, Automation and OT Cybersecurity Awareness: Co

Learning objectives

- Explain digital oilfield, automation and ot cybersecurity awareness: competence review, interpret a case, select appropriate controls and justify a documented decision.

Lessons

1. Purpose and key terms of Digital Oilfield, Automation and OT Cybersecurity Awareness: Competence Review
2. Systems and operating context
3. Evidence, assumptions and decision gates
4. Hazards, safeguards and escalation
5. Applied case: Digital Oilfield, Automation and OT Cybersecurity Awareness

Detailed teaching notes

Teaching notes

Core explanation. Digital Oilfield, Automation and OT Cybersecurity Awareness: Competence Review describes a practical part of Digital Oilfield, Automation and OT Cybersecurity Awareness. 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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 digital oilfield, automation and ot cybersecurity awareness: 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.