



Cybersecurity and Enterprise Resilience

DURATION

5 days

CONTACT HOURS

30

LEVEL

Intermediate

FEE PER DELEGATE

US\$1,500

Defending an organisation that cannot be made secure, and continuing to operate once something has got through.

Security programmes fail in a predictable way: controls are bought, the inventory is incomplete, and nobody has tested what happens when an attacker is already inside. Resilience is the other half and usually the weaker one, because recovery plans are written once and never exercised against a scenario in which the recovery systems are themselves affected. This week treats the two together, from identifying what the organisation cannot operate without to running an incident and getting back. Delegates work from their own environment and leave with a tested plan rather than a document.

Available as classroom, live online, in house.

Who it is for

Information security managers and officers, IT managers responsible for infrastructure and recovery, risk and continuity managers, and internal auditors reviewing security.

What you will be able to do

- Identify what the organisation cannot operate without, and what depends on it.
- Prioritise controls against the way attacks actually arrive rather than against a checklist.
- Detect an intrusion that is already inside the perimeter.
- Run an incident with a defined command structure, including the decisions nobody wants to take.
- Test a recovery plan against a scenario where the recovery systems are affected.

The outline

DAY 1

What is actually being defended

Asset and dependency inventory, and why it is always incomplete · What the organisation cannot operate without, and for how long · Threats this organisation faces, not threats in general · Accepting that some compromise is certain

DAY 2

Controls worth the money

Identity, patching and backup, and why they stay first · Segmentation, so one compromise is not every compromise · A framework as a checklist against a framework as a plan · Third parties, and the access nobody is tracking

DAY 3

Detection

Assuming presence, and looking for it · Logging that would show what you need afterwards · Alert volume, and the backlog problem · Exercising detection rather than assuming it works

DAY 4

Running an incident

Command, roles and who is allowed to decide · Containment against preserving evidence · Communicating internally, to customers and to a regulator · The hardest decisions, taken in advance

DAY 5

Getting back

Recovery when the recovery systems are affected · Order of restoration, and the dependencies that dictate it · Testing against a scenario rather than reading the plan · What to change afterwards, and proving it changed

What you leave with

- A dependency map of the delegate's critical services, with single points of failure named.
- A prioritised control plan tied to the threats the organisation actually faces.
- An incident response and recovery plan with roles, thresholds and a tested escalation path.

Published dates

DATES	WHERE	FEE
23 to 27 November 2026	Dar es Salaam, Tanzania	US\$1,500
30 November 2026 to 4 December 2026	Accra, Ghana	US\$1,500
7 to 11 December 2026	Nairobi, Kenya	US\$1,500
14 to 18 December 2026	Dubai, United Arab Emirates	US\$1,500

Fees are per delegate and cover travel and accommodation arranged by the delegate. Registration fees are not included.

Register or ask a question

globalaxistraining.co.za/courses/cybersecurity-and-enterprise-resilience
info@globalaxistraining.co.za
+27 72 337 9234

250 Beyers Naude Drive, Rustenburg, North West, 2999, South Africa

This copy was produced on 30 October 2026.