GSDC
Global Skill Development Council

FIELD GUIDE · CISO31K · ISO 31000:2018

Maya's Full Field Guide

From internal audit analyst at **$94K** to a certified ISO 31000 Risk Manager at **$148K** — in 90 days. This is the complete playbook she followed, and the reference she still keeps open at work.

Salary guide | Career roadmap | AI governance roles | Hiring trends

Inside the AI Compliance Toolkit — a 20-page reference

The 5-chapter story + 6-module syllabus map + every artifact she shipped. The risk management certification reference CISO31K alumni keep open at work.

- 5-chapter narrative + module map
- Risk register + risk matrix + risk heat map templates
- Bowtie analysis + risk treatment plan example
- ISO 31000 audit checklist (Module 6)
- Top-100 ISMS non-conformities reference

A GSDC reference guide for current and aspiring risk professionals.

GSDC
Global Skill Development Council

THE 5-CHAPTER STORY · PART ONE

How an audit analyst became a risk manager

Maya's story is the spine of this guide. Each chapter maps to a real capability you build inside CISO31K — so the narrative doubles as a study path.

01

The $94K ceiling

Maya was a strong internal audit analyst, but her risk work was ad hoc: spreadsheets, gut feel, and findings that landed too late to change decisions. Without a recognised framework, she could flag problems — but she couldn't *own* risk. The salary band for "analyst" capped what the work could become.

02

Finding ISO 31000

She discovered that ISO 31000:2018 gives organisations a single, defensible language for risk — principles, framework, and a repeatable process. The **Certified ISO 31000 Risk Manager (CISO31K)** credential from GSDC packaged that language into six modules and 16+ hours of guided learning, with the exact templates practitioners use. She enrolled the same week.

> *"The framework didn't just teach me risk — it gave me the vocabulary to be trusted with it."*
>
> **— Maya, on Module 1**

THE 5-CHAPTER STORY · PART TWO

90 days, six modules, one new title

03

The 90-day sprint

Maya worked through the six modules in evenings and weekends — roughly 16 focused hours of content plus practice. She didn't just watch; she rebuilt each artifact against her own employer's risks, turning the course into a live portfolio.

04

The toolkit at work

Her risk register replaced three disconnected spreadsheets. Her heat map gave leadership a one-glance view of exposure. A bowtie analysis on a key vendor dependency turned a vague worry into a funded mitigation plan. Suddenly she was in the room where decisions were made.

05

The $148K risk manager

Within a quarter, Maya moved from **audit analyst ($94K)** to **ISO 31000 Risk Manager ($148K)** — a step change driven less by tenure than by a credential and a portfolio that proved she could run the risk process end to end.

GSDC
Global Skill Development Council

SALARY GUIDE & CAREER ROADMAP

What the title is worth — and how you get there

Indicative annual base ranges for risk roles in mature markets. Bands vary by region, sector, and scope; treat them as direction, not promise.

Role	Typical base range	Core signal employers want
Internal Audit / Risk Analyst	$80K – $100K	Controls testing, findings
Risk Specialist	$95K – $120K	Risk register ownership
ISO 31000 Risk Manager	**$135K – $160K**	Runs the full risk process
Lead / ERM Manager	$155K – $185K	Enterprise framework, board reporting
Head of Risk / CRO track	$190K +	Strategy, appetite, assurance

The roadmap in five moves

1. **Analyst** — Learn controls & findings
2. → **Specialist** — Own a risk register
3. → **ISO 31000 Manager** — CISO31K + portfolio
4. → **ERM Lead** — Enterprise framework
5. → **Head / CRO** — Risk strategy

LIMITED TIME

Move up a band, not just a step

The credential that separates “flags risk” from “owns risk” on a resume.

Enroll while it’s open →

GSDC
Global Skill Development Council

AI GOVERNANCE ROLES & HIRING TRENDS

Where risk management is heading next

AI has created a new tier of risk roles — and they speak the language of ISO 31000. The same process that governs operational risk now governs models, data, and automated decisions.

Emerging AI governance roles

- ✓ AI Risk Manager
- ✓ AI Governance & Assurance Lead
- ✓ Model Risk Officer
- ✓ Responsible-AI Compliance Manager
- ✓ Data & Algorithmic Risk Partner

What hiring managers screen for

- ✓ A recognised risk framework (ISO 31000)
- ✓ Ability to run risk assessment + treatment
- ✓ Heat maps & registers leadership can read
- ✓ Audit / assurance literacy
- ✓ Mapping controls to AI-specific threats

Hiring trends at a glance

Rising
Demand for governance roles that pair AI with a formal risk framework

Cross-over
ISO 31000 skills transfer directly to AI & model risk

Premium
Framework-certified candidates shortlist faster

VALID 48 HOURS

Be ready before the role is posted
ISO 31000 is the base layer under almost every AI governance job description.

Reserve your spot →

GSDC
Global Skill Development Council

THE 6-MODULE SYLLABUS MAP

Every module, and the artifact it produces

16+ hours of guided learning. Each module ends with something you can ship at work — the “artifacts Maya shipped” come from here.

M1 — **Foundations of Risk & ISO 31000:2018**
Concepts, vocabulary, why a framework matters. **Artifact: risk vocabulary baseline.**

M2 — **Principles, Framework & Leadership**
The 8 principles, governance, integrating risk into decisions. **Artifact: framework charter.**

M3 — **The Risk Management Process / Lifecycle**
Scope, context, criteria; the end-to-end cycle. **Artifact: process map.**

M4 — **Risk Assessment Techniques**
Identification, analysis, evaluation. **Artifacts: risk register, matrix, heat map.**

M5 — **Risk Treatment, Bowtie & ERM**
Options, controls, residual risk, enterprise integration. **Artifacts: bowtie, treatment plan.**

M6 — **Monitoring, Audit & Assurance**
Review, reporting, conformity. **Artifacts: audit checklist, non-conformity log.**

50% OFF

Six modules, one portfolio
Finish CISO31K with artifacts you can show in an interview, not just a certificate.

Begin Module 1 →

ARTIFACTS SHE SHIPPED · TEMPLATES

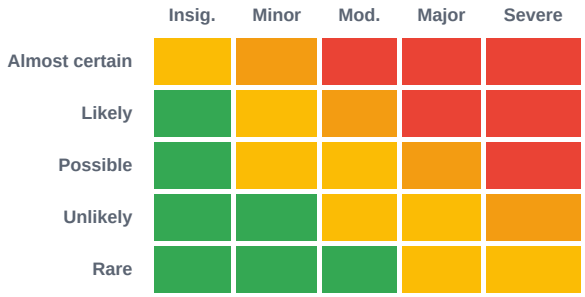
Risk register, risk matrix & heat map

These three artifacts turned Maya's scattered notes into a system leadership could read in seconds. Here is the shape of each.

1 · Risk register (column blueprint)

ID	Risk	Cause	Likelihood	Impact	Owner	Treatment	Residual
R-01	Vendor outage	Single supplier	Possible	Major	Ops	Add backup	Low
R-02	Data breach	Weak access ctrl	Unlikely	Severe	Security	MFA + review	Medium

2 · Risk matrix (5×5)



3 · Heat map legend

- Low — monitor, accept
- Medium — manage actively
- High — treat, assign owner
- Extreme — escalate now

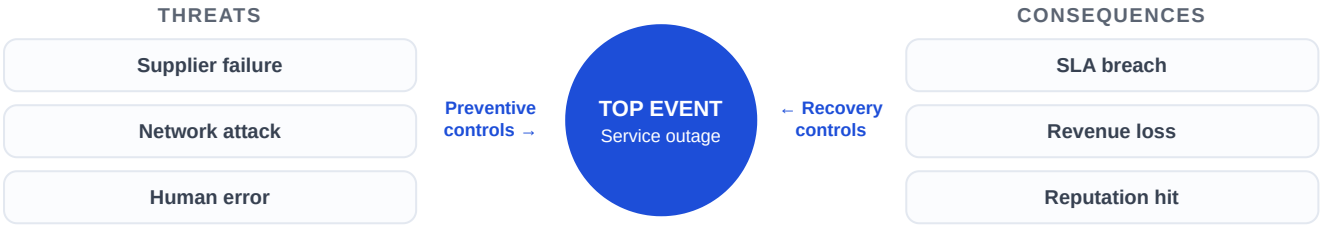
The matrix and heat map share one colour scale, so a register row, a grid cell, and a board slide all tell the same story.

GSDC
Global Skill Development Council

BOWTIE ANALYSIS & RISK TREATMENT PLAN

From a single event to a funded plan

A bowtie puts one risk event in the centre, threats on the left, consequences on the right, and controls on the strings between them.



Risk treatment plan (worked example)

Risk	Option	Action	Owner	Due	Residual
Vendor outage	Reduce	Onboard second supplier	Procurement	Q2	Low
Data breach	Reduce	Enforce MFA, quarterly access review	Security	Q1	Medium
Key-person loss	Share	Cross-train + document runbooks	Eng Lead	Q3	Low

MODULE 6 · AUDIT & ASSURANCE

The audit checklist & the non-conformity reference

Module 6 is the one alumni keep open at work — assurance is where a risk manager proves the framework is actually running.

ISO 31000 audit checklist (sample items)

- ✓ Is risk criteria documented & approved?
- ✓ Is the register current and owned?
- ✓ Are treatments tracked to closure?
- ✓ Is residual risk within appetite?
- ✓ Is risk reported to leadership on cadence?
- ✓ Are controls tested for effectiveness?
- ✓ Is the framework reviewed periodically?
- ✓ Are lessons fed back into the process?

Top-100 ISMS non-conformities reference

A curated catalogue of the most common findings auditors raise — grouped so you can pre-empt them before an assessment. Representative categories:

#	Category	Typical finding
01–20	Documentation & scope	Outdated or missing risk criteria
21–45	Risk assessment	Register not maintained; no owners
46–70	Treatment & controls	Actions overdue; effectiveness untested
71–90	Monitoring & review	No periodic management review
91–100	Reporting & assurance	Inconsistent leadership reporting