GSDC
Global Skill Development Council

FRAMEWORK REFERENCE · ISO 31000:2018 · CISO31K

The Full Framework Reference

The complete ISO 31000 reference, in annotated diagrams — the **8 principles**, the **framework cycle**, the **3-step process**, the ERM and governance layers, and how it compares to COSO and ISO 27005. The page CISO31K alumni keep open.

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

Inside this reference

Everything you need to read, draw and explain ISO 31000 from memory — the structure interviewers probe and the model you'll run at work.

- ISO 31000 framework diagrams (annotated)
- 8 Principles full reference
- 3-step process + sub-steps
- ERM + governance layers
- ISO 31000 vs COSO vs ISO 27005

A GSDC reference guide. Diagrams interpret ISO 31000:2018; consult the standard for the authoritative text.

GSDC
Global Skill Development Council

THE BIG PICTURE · HOW THE STANDARD FITS TOGETHER

ISO 31000 on one map

The standard has three connected parts. Principles say *why*; the framework says *how the organisation is set up*; the process says *what you do to a risk*.

Principles

8 principles that keep risk management effective and centred on **value creation & protection**.

WHY

\+

Framework

6 components, led by leadership & commitment, that embed risk into governance and decisions.

HOW SET UP

\+

Process

The repeatable steps applied to each risk — scope, assess, treat — with monitoring throughout.

WHAT YOU DO

All three serve one purpose: **the creation and protection of value.**

How to use this reference

To learn

- ✓ Read each diagram, then redraw it from memory
- ✓ Tie every box to a real risk you know

To apply

- ✓ Run the process; govern with the framework
- ✓ Check decisions against the 8 principles

50% OFF

Learn the whole model, not fragments

CISO31K teaches this map end-to-end — the certification employers screen for, at half price.

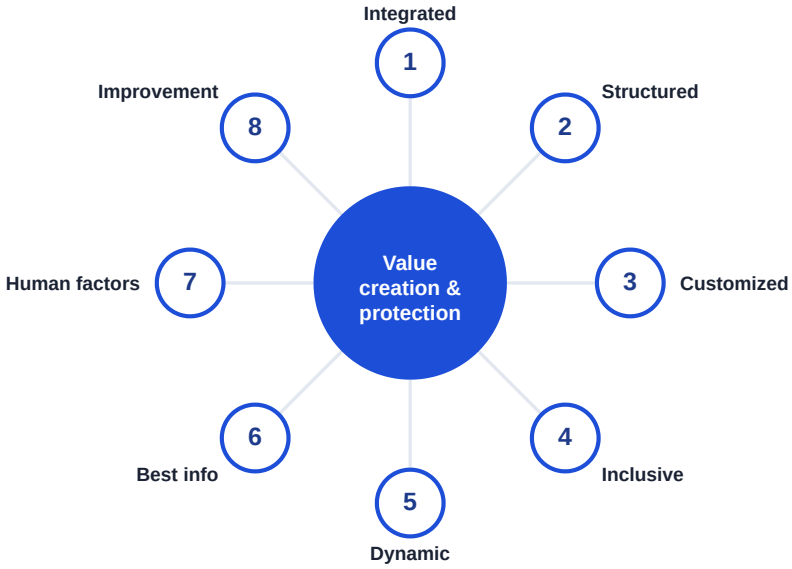
Get certified →

GSDC
Global Skill Development Council

THE 8 PRINCIPLES · FULL REFERENCE

Eight principles around one purpose

Every principle points back to the core: creating and protecting value. The numbers in the wheel map to the table below.



#	Principle	What it means in practice
1	Integrated	Part of all activities, not a side process
2	Structured & comprehensive	A consistent approach gives reliable results
3	Customized	Scaled to the organisation's context & objectives
4	Inclusive	Stakeholders involved; knowledge & views considered
5	Dynamic	Anticipates and responds to change
6	Best available information	Uses historical, current & expected data — with its limits
7	Human & cultural factors	Behaviour & culture shape risk at every step
8	Continual improvement	Improves through learning & experience

50% OFF TODAY

Recite all eight in an interview

CISO31K drills the principles until they're second nature — enrollment is 50% off today.

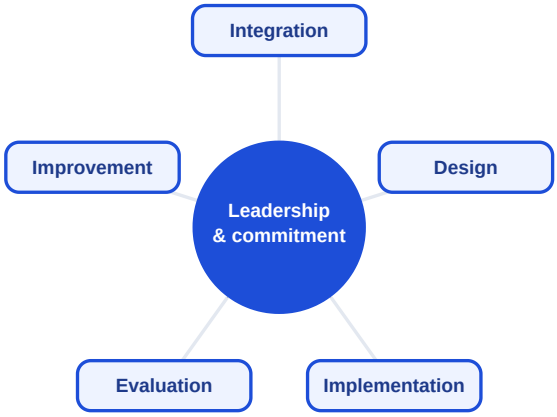
Claim 50% off →

GSDC
Global Skill Development Council

THE FRAMEWORK · 6 COMPONENTS

The cycle that embeds risk in the organisation

The framework is how risk management lives inside governance. Leadership & commitment sits at the centre; the other five components run as a continual improvement cycle around it.



Component	Role
Leadership & commitment (core)	Mandate, accountability, alignment to objectives
Integration	Embed risk into governance & all functions
Design	Understand context; set policy, roles, resources
Implementation	Put the plan into action across the organisation
Evaluation	Measure performance against purpose
Improvement	Adapt and continually improve the framework

LIMITED TIME

Draw the framework from memory
Being able to sketch this cycle on a whiteboard is what separates certified candidates.

Enroll while it's open →

GSDC
Global Skill Development Council

THE PROCESS · 3 CORE STEPS + SUB-STEPS

What you actually do to a risk

Three core steps, wrapped by continuous activities. Communication runs across the top, monitoring across the bottom, and everything is recorded and reported.

Communication & consultation — throughout

STEP 1
Scope, context & criteria
Define scope · external/internal context · risk criteria

→

STEP 2
Risk assessment
Identification → Analysis → Evaluation

→

STEP 3
Risk treatment
Select options · plan · implement · check residual

Monitoring & review — throughout · Recording & reporting

Step 2 in detail — the three sub-steps

Sub-step	Question	Output
Identification	What could happen, and why?	Risk register entries
Analysis	How likely, and how severe?	Likelihood × impact scores
Evaluation	Is it within our criteria?	Treat / tolerate decision

VALID 48 HOURS

Run the process, don’t just name it
CISO31K turns these steps into artifacts you can show — reserve your seat in the next 48 hours.

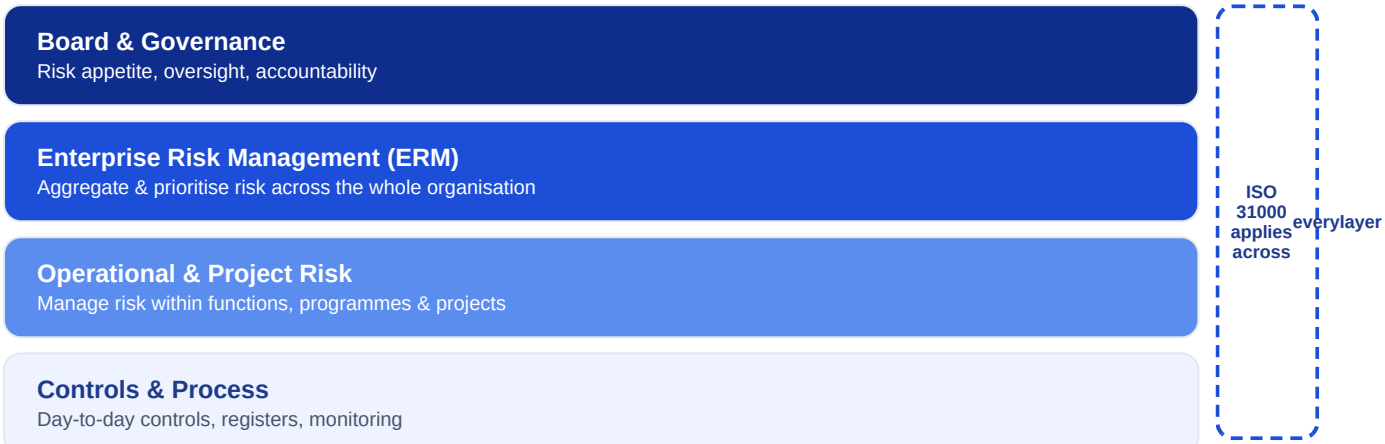
Reserve your spot →

GSDC
Global Skill Development Council

ERM + GOVERNANCE LAYERS

Where ISO 31000 sits in the organisation

Risk management is not one team's job. ISO 31000 spans every layer — from the boardroom mandate down to day-to-day controls.



The governance overlay

Top-down

- ✓ Board sets appetite & tolerance
- ✓ ERM translates it into priorities

Bottom-up

- ✓ Controls surface real exposure
- ✓ Reporting rolls risk back to the board

RELATED

Speak to every layer with confidence

From control owner to CRO, ISO 31000 is the shared language — CISO31K teaches it.

Start learning →

GSDC
Global Skill Development Council

STANDARDS COMPARED

ISO 31000 vs COSO ERM vs ISO 27005

Three standards people confuse. Here is what each is for — and where ISO 31000 is the right starting point.

Dimension	ISO 31000	COSO ERM	ISO 27005
Focus	Risk of any kind	Enterprise risk & strategy	Information security risk
Nature	Principles-based guidance	Control & entity framework	InfoSec risk process
Scope	Any organisation, any risk	Whole enterprise	Within an ISMS (ISO 27001)
Structure	Principles · framework · process	5 components · 20 principles	Aligned to ISO 31000 process
Best for	A universal risk foundation	US-listed / strategy-led ERM	Security & compliance teams

How they relate

- ✓ ISO 27005 follows the ISO 31000 process for InfoSec
- ✓ COSO & ISO 31000 can coexist; many firms map one to the other
- ✓ ISO 31000 is the broadest, most transferable base

Where to start

- ✓ Learn ISO 31000 first — it underpins the others
- ✓ Add COSO for strategy/board context
- ✓ Add ISO 27005 for security specialisation

TOOLKIT INCLUDED

Know which standard, and when

CISO31K makes you fluent in ISO 31000 and how it maps to COSO and ISO 27005.

Unlock the program →

GSDC
Global Skill Development Council

PUTTING IT TOGETHER · A WORKED WALKTHROUGH

One risk, through the whole framework

Watch a single risk — a critical vendor outage — move through every part of the model you've just seen.

Stage	What happens to "vendor outage"
Principles	Use best available info; involve stakeholders; keep it dynamic
Framework	Leadership mandates vendor-risk oversight; integrated into procurement
Scope & criteria	Scope = critical suppliers; criteria = max tolerable downtime
Identification	Single-supplier dependency logged as R-01
Analysis	Possible × Major = High on the matrix
Evaluation	Above appetite — must be treated
Treatment	Onboard a second supplier; residual = Low
Monitor & report	KRI tracked; status reported to the board quarterly

From principle to board report, **one consistent thread** — that thread is ISO 31000.

SEATS FILLING

Practice the walkthrough until it's yours

CISO31K runs end-to-end walkthroughs like this on real risks. Seats are filling.

Hold my seat →

GSDC
Global Skill Development Council

WHY THIS REFERENCE PAYS OFF · SALARY · CAREER · AI · HIRING

The reference behind the credential

Fluency in this framework is what the certification certifies — and what moves a career. Here is the payoff.

Salary & career

- ✓ Median alumni report a +47% salary lift
- ✓ Risk Manager national avg ~$163K
- ✓ Path: Analyst → Manager → ERM → CRO
- ✓ Framework fluency signals you can lead risk

AI governance & hiring

- ✓ ISO 31000 is the base layer for AI risk roles
- ✓ 7,000+ open USA risk roles right now
- ✓ Certified candidates shortlist faster
- ✓ Risk + AI literacy commands a premium

From reference to results

Learn — This framework, cold → **Certify** — CISO31K credential → **Advance** — Better roles & pay

FINAL CALL · 50% OFF

Master the framework. Earn the credential.

CISO31K is the ISO 31000 certification employers screen for — at 50% off, while the offer lasts.

Certify with CISO31K →