



CBA STANDARD

Compliance & Risk Professional

Management · 5 weighted domains · 29 learning objectives

Version 7.1

This edition published September 2026

About this standard

This standard defines what competent practice consists of in the discipline set out under Scope below. It divides the discipline into weighted domains and states, for each domain, the learning objectives a competent practitioner meets. It is one of the CBA Standards, which the Corporate Business Alliance maintains across finance, accounting, management and technology.

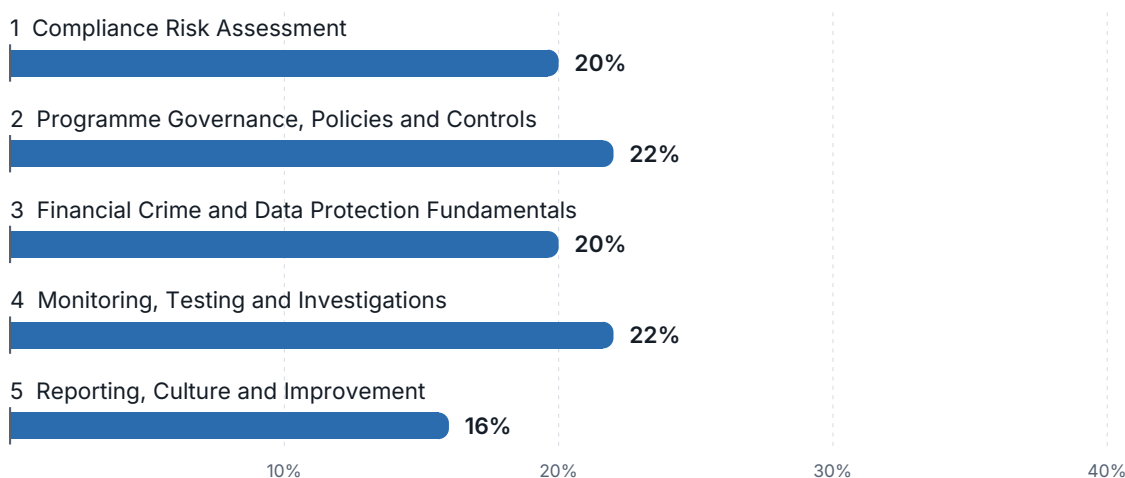
The standard is written for employers defining what a role requires, for training providers designing courses to a published specification, and for practitioners planning their own development.

Each domain carries a weight: its share of the standard, and of the examination for the CBA-CRP credential, which is assessed against it. The version number rises whenever a change would alter what competence in the discipline means, and every credential records the version its holder met.

Scope

The CBA Certified Compliance & Risk Professional (CBA-CRP) validates the ability to build and run a complete compliance programme: assessing risk, writing policies and controls, monitoring, handling investigations, and reporting to leadership. Jurisdiction-neutral and concept-focused.

Weighting by domain



Domains and learning objectives

Domain 1

20% of the standard

Compliance Risk Assessment

- 1.1 Identify sources of compliance obligation and translate them into an inventory of organisational risks
- 1.2 Calculate inherent and residual risk scores using likelihood and impact scales, and justify the scale design
- 1.3 Distinguish inherent risk, residual risk, risk appetite and risk tolerance in practical scenarios
- 1.4 Prioritise risks for treatment and select an appropriate treatment response (accept, mitigate, transfer, avoid)

- 1.5 Evaluate the quality of a risk register entry and identify missing or defective elements
- 1.6 Interpret changes in an organisation's risk profile triggered by new products, markets, suppliers or technology

Domain 2

22% of the standard

Programme Governance, Policies and Controls

- 2.1 Select an appropriate governance structure for a compliance programme given organisational size and risk profile
- 2.2 Distinguish the responsibilities of operational management, compliance functions and independent assurance within a layered defence model
- 2.3 Evaluate a draft policy against criteria of clarity, scope, ownership, proportionality and enforceability
- 2.4 Differentiate preventive, detective and corrective controls and match control types to identified risks
- 2.5 Design a training and communication approach that targets the right audiences with the right depth
- 2.6 Assess whether a described programme element is proportionate to the organisation's size and risk exposure

Domain 3

20% of the standard

Financial Crime and Data Protection Fundamentals

- 3.1 Explain the three-stage model of money laundering and identify the stage illustrated by a described transaction pattern
- 3.2 Distinguish customer due diligence, enhanced due diligence and ongoing monitoring, and select the appropriate level for a given customer profile
- 3.3 Identify red flags for money laundering, bribery and sanctions exposure in workplace scenarios
- 3.4 Interpret core data-protection concepts including personal data, lawful processing purposes, data minimisation and retention
- 3.5 Select the correct first response when a possible data breach or suspicious activity is discovered
- 3.6 Evaluate third-party relationships for financial crime and data-protection risk at a conceptual level

Domain 4

22% of the standard

Monitoring, Testing and Investigations

- 4.1 Distinguish continuous monitoring, periodic testing and independent review, and select which is appropriate for a given assurance need
- 4.2 Design a risk-based monitoring plan including sample selection, frequency and pass criteria
- 4.3 Interpret monitoring results to distinguish an isolated error from a control weakness or systemic failure
- 4.4 Evaluate alert-based monitoring output, including tuning thresholds and managing false

positives, whether rule-based or AI-assisted

- 4.5 Select sound practice for the intake, triage and initial handling of a whistleblowing report or suspected breach
- 4.6 Apply core investigation principles: preserving evidence, maintaining confidentiality, fairness to subjects and documenting steps

Domain 5

16% of the standard

Reporting, Culture and Improvement

- 5.1 Select metrics and key risk indicators that give leadership a faithful picture of compliance performance
- 5.2 Construct a management report from raw programme data, choosing appropriate structure, emphasis and visualisation
- 5.3 Interpret indicators of compliance culture, including speak-up data, and diagnose likely cultural weaknesses from a scenario
- 5.4 Distinguish activity metrics from outcome metrics and evaluate a dashboard for balance between them
- 5.5 Evaluate lessons-learned and programme review processes and select improvements after an incident or audit finding

Competence at award

What a holder of the CBA-CRP credential has demonstrated.

- Design and populate a compliance risk assessment, scoring likelihood and impact and prioritising risks against a stated risk appetite
- Draft the core elements of a compliance programme: governance structure, policy framework, controls and training aligned to identified risks
- Explain the purpose and typical mechanics of anti-money-laundering and data-protection regimes at a conceptual, jurisdiction-neutral level
- Plan and execute monitoring and testing activity, interpret the results and distinguish control weaknesses from isolated errors
- Triage reports of suspected misconduct and apply sound practice in the opening stages of an internal investigation
- Build management reporting on compliance performance using accessible tools such as Excel or Google Sheets
- Assess the health of an organisation's compliance culture and select realistic interventions to strengthen it

Recognition at Professional level

The CBA-CRP credential is awarded at Professional level of the CBA Competency Framework, which evidences that the holder is a practising professional in the discipline.

Awarded on the examination, 6 assessed workbooks of applied work and 3 years' relevant

professional experience (2 with a relevant degree), confirmed by a named referee, with a signed undertaking to the Code of Professional Conduct.

Who the standard is written for

Early-career compliance and risk staff

Analysts, officers and coordinators in compliance, risk, audit or legal support roles who want a structured, recognised foundation covering the whole programme cycle rather than one narrow speciality.

Operations and finance professionals moving into compliance

Professionals in operations, finance, HR or customer onboarding who already apply controls day to day and want to formalise that experience into a dedicated compliance and risk career path.

Managers accountable for compliance in smaller organisations

Owners, general managers and department heads in SMEs, startups and regional firms who carry compliance responsibility without a large specialist team and need to build a proportionate programme themselves.

Appendix: glossary of management terms

Terms used across the management standards, as CBA defines them.

Anti-money laundering (AML)

The laws, controls and procedures designed to prevent the proceeds of crime being disguised as legitimate funds, including customer due diligence, monitoring and reporting of suspicion.

Assurance

An objective examination that gives a stated level of confidence that a process, control or report works as intended.

Attribution model

A rule or algorithm for sharing credit for a conversion among the marketing touches in a customer's journey: last-click, first-click, linear, position-based, time-decay or algorithmic. None is a controlled test of which conversions would have happened without the spending.

Bottleneck

The step in a process with the least capacity relative to demand. It limits the output of the whole process, so improvement elsewhere does not raise throughput.

Break-even ROAS

The return on ad spend at which contribution from attributed sales covers the advertising: one divided by the contribution margin rate. The rate is net of payment and delivery costs, returns, discounts and every other variable cost except the advertising.

Business continuity plan

A documented plan for keeping critical activities running, or restoring them within set times, after a disruption.

Campaign tracking parameters

Labels appended to a link telling analytics which source, medium, campaign and ad sent a visit. A spelling or case difference splits a campaign into several, so links follow a naming convention and are fixed at source, not in reports.

Capacity

The maximum output a process, resource or organisation can produce in a period under normal conditions.

Capacity utilisation

Actual output as a percentage of capacity. Running close to full utilisation lengthens queues and lead times sharply.

Category management

Managing a group of related purchases as a single strategic unit, with a plan based on the organisation's demand and the supply market for that category.

Change management

The structured approach to moving people and processes from a current state to a new one, so that the change is adopted and sustained.

Claim substantiation

Holding evidence, before publication, that supports a factual, comparative, price or environmental claim as it is worded. That competitors make the same claim is not evidence, and evidence about one component does not support a claim about the whole product.

Click-through rate (CTR)

Clicks as a percentage of impressions. In organic search, a fall in CTR while position holds can mean the results page is answering the query itself, though more ads above the result or a changed snippet can do the same.

Compliance

Conformity with the laws, regulations, internal policies and contractual obligations that apply to an organisation.

Compliance risk

The risk of legal or regulatory sanction, financial loss or reputational damage from failing to comply with applicable rules.

Conflict of interest

A situation in which a personal interest could influence, or appear to influence, the performance of a professional duty. It is managed by disclosure and, where needed, by removing the person from the decision.

Contract management

Managing a contract after award so that both parties meet their obligations and the intended value is delivered, including performance monitoring, variations and closure.

Control

In risk management, an action, process or mechanism that reduces the likelihood or impact of a risk.

Control environment

The attitudes, structures and standards across an organisation that set the tone for how controls are designed and followed.

Conversion rate (CVR)

Conversions as a percentage of the clicks, visits or users that could have converted, with the base named, since each gives a different figure. A funnel stage's rate is the users completing it divided by those who reached it.

Corrective action

Action taken to remove the cause of a detected problem so that it does not recur, as distinct from correcting the problem itself.

Cost per click (CPC)

Advertising spend divided by the number of clicks it bought. For a lead goal, the most that can be paid per click is the target cost per lead multiplied by the conversion rate per click.

Cost per thousand impressions (CPM)

Advertising spend divided by impressions, multiplied by 1,000. Impressions include repeat showings to the same person, so CPM is not the cost of reaching a thousand people, which is spend divided by reach, multiplied by 1,000.

Creative fatigue

The decline in response to an ad as the same people see it repeatedly, which fresh creative shown to the same audience restores. In audience saturation, by contrast, reach stops growing and only a new audience restores response.

Customer acquisition cost (CAC)

The cost of winning one new customer: marketing and sales cost in a period divided by the new customers won in it. The highest affordable CAC is the contribution a new customer earns within the payback period

the business sets.

Cycle time

The time taken to complete one unit of work from start to finish in a process.

Deliverability

The ability of a sender's messages to reach the inbox rather than being blocked or filtered as spam. Bounce, complaint and click rates indicate it; delivery rate counts mail filed as spam, and automatic image loading can inflate open rates.

Due diligence

A structured investigation undertaken before a decision — appointing a supplier, onboarding a customer, making an acquisition — to identify risks and verify claims.

Economic order quantity (EOQ)

The order size that minimises the combined cost of ordering and holding inventory, calculated as the square root of twice annual demand times the cost per order, divided by the annual holding cost per unit.

Engagement rate

Engagements, counting specified actions such as likes, comments, shares and saves, as a percentage of reach. A rate worked on followers or impressions is a different figure, so two rates compare only when the actions counted and the base match.

Escalation

Referring an issue to a higher level of authority under defined criteria, so that it is decided by someone with the authority to act.

Five whys

A root cause technique that asks "why" repeatedly, each answer forming the basis of the next question, until the underlying cause is reached.

Frequency

In advertising, the average number of times each person reached was shown an ad in a period: impressions divided by reach. Rising frequency with falling click-through fits both creative fatigue and audience saturation, so on its own it shows neither.

Governance

The system of rules, roles and processes by which an organisation is directed and controlled, including who decides what and how they are held to account.

Incrementality

The conversions that marketing caused, over and above those that would have happened without it, measured against a randomly held-out group or matched control regions. Platform- and retailer-reported conversions, by contrast, can include sales that would have happened anyway.

Inherent risk

The level of a risk before any controls are applied.

Internal audit

An independent function that provides assurance to the board on whether governance, risk management and controls are effective.

Inventory turnover

Cost of sales divided by average inventory, showing how many times inventory is sold and replaced in a period.

Invitation to tender (ITT)

A formal request to suppliers to submit a bid against a defined specification, terms and evaluation criteria.

Kaizen

Continuous improvement through frequent small changes, typically led by the people who do the work.

Key risk indicator (KRI)

A measure that signals rising exposure to a risk, with thresholds that trigger review or escalation before the risk crystallises.

Know your customer (KYC)

Verifying the identity of customers and understanding the nature of their business and the source of their funds, as part of anti-money laundering controls.

Lead scoring

Awarding leads points for fit and behaviour, such as job role and pages visited, so that those above a threshold pass to sales. The threshold matches sales capacity, passing the best leads sales can promptly follow up, not the most.

Lead time

The total time from a request or order to its delivery, including waiting time as well as processing time.

Lean

A management approach that improves flow and value to the customer by systematically removing waste from processes.

Lifetime value (LTV)

The contribution a customer is expected to generate over the whole relationship, worked from margin per order, purchase frequency and retention rather than revenue. Also called customer lifetime value (CLV), it caps what is worth paying to acquire a customer.

Marketing consent

A person's recorded agreement, given freely by positive action, to receive marketing from an identified sender through a named channel. Pre-ticked boxes, bundled consent and a list seller's generic consent do not count; when consent is required varies by market.

Marketing mix modelling (MMM)

A statistical model that estimates each channel's contribution to sales, offline channels included, from aggregate spend and sales over time, not individual journeys. It models carry-over, where advertising keeps working after it stops, and saturation, where extra spend returns less.

Maverick spend

Purchasing that bypasses agreed contracts, approved suppliers or procurement procedures.

Negative keyword

A word or phrase that stops a paid search campaign or ad group showing ads for queries that match it, such as job-seeking or wrong-language searches. Negatives are set at launch, then added from the search terms report.

Policy

A statement of what an organisation requires and why, approved at an appropriate level. A procedure sets out how the policy is carried out.

Process mapping

Drawing the steps, decisions, handoffs and roles in a process, so that delays, duplication and control gaps

become visible.

RACI matrix

A chart assigning, for each task or decision, who is Responsible, Accountable, Consulted and Informed.

Reorder point

The inventory level at which a new order is placed: expected demand during the supply lead time plus safety stock.

Request for information (RFI)

An early approach to the market to learn about possible suppliers and solutions before a requirement is finalised.

Request for quotation (RFQ)

A request to suppliers for prices against a clearly defined requirement, typically used where price is the main differentiator.

Residual risk

The level of a risk remaining after controls are applied. It is compared with risk appetite to decide whether further action is needed.

Return on ad spend (ROAS)

Attributed revenue divided by the advertising spend it is attributed to. It measures revenue, not profit: attributed sales cover their advertising only when ROAS reaches break-even ROAS, with both on one revenue basis, such as net of VAT and returns.

Risk appetite

The amount and type of risk an organisation is willing to accept in pursuit of its objectives, approved by its board.

Risk matrix

A grid that scores risks by likelihood and impact, often coloured as a heat map, to prioritise attention. Its scores are judgements and should be read as such.

Risk register

A record of identified risks with their causes, owners, ratings, controls and actions, reviewed regularly.

Root cause analysis

A structured method for identifying the underlying cause of a problem, rather than its symptoms, so that corrective action prevents recurrence.

Safety stock

Inventory held above expected demand to protect against variation in demand or supply lead time.

Sanctions screening

Checking customers, suppliers and transactions against government sanctions lists before dealing with them.

Search engine optimisation (SEO)

Improving a site's visibility in unpaid search results through crawlable, indexable pages matched to the intent behind queries, original content and links earned rather than bought. Search engines' published spam policies prohibit links bought to pass ranking credit.

Search intent

The purpose behind a search query, usually classed as informational, navigational, commercial or transactional. Each query, in any language, dialect or script, is matched to the page type that serves its

purpose, such as a guide for a question.

Service level agreement (SLA)

A defined, measurable standard of service a supplier or internal team commits to, such as response time or availability, with the consequences of missing it.

Six Sigma

A data-driven improvement method that reduces variation and defects, typically following the DMAIC cycle: define, measure, analyse, improve, control.

Specification

The statement of what is required from a supplier. A technical specification describes the product or method; an output-based specification describes the result to be achieved.

Spend analysis

Collecting, cleaning and classifying an organisation's purchasing data to show what is bought, from whom and at what cost, as the basis for category strategies.

Stakeholder

A person or group who affects, or is affected by, a decision, project or organisation.

Standard operating procedure (SOP)

A written, step-by-step instruction for carrying out a routine activity consistently.

Supplier relationship management

A structured approach to managing interactions with important suppliers to improve performance, reduce risk and develop value over time.

Supply positioning

Classifying purchases by their value to the organisation and the risk in their supply market — often shown as the Kraljic matrix — to choose a sourcing approach for each.

Suppression list

A list of contacts never to be messaged or uploaded to ad platforms, such as those who unsubscribed, complained or hard-bounced, checked before every send and upload. Opted-out contacts are suppressed, not deleted, so a later import cannot restore them.

Tender evaluation criteria

The weighted criteria against which bids are scored, fixed and published before bids are opened so that the evaluation cannot be shaped to a preferred bidder.

Three lines model

A governance model, published by the Institute of Internal Auditors, that distinguishes management's ownership of risk (first line), specialist risk and compliance oversight (second line) and independent assurance by internal audit (third line).

Throughput

The rate at which a process produces finished output, set by its bottleneck.

Total cost of ownership (TCO)

The full cost of acquiring, operating, maintaining and disposing of an asset or service over its life, not only its purchase price.

Transcreation

Adapting marketing copy into another language so that its intent, tone and effect survive, rewriting idiom, humour and cultural references rather than translating them word for word. Regulated wording, such as

offer terms, prices and legal statements, is translated exactly.

Value stream map

A diagram of every step, delay and information flow needed to deliver a product or service, used to separate value-adding time from waste.

Waste

In lean practice, any activity that consumes resources without adding value for the customer, such as waiting, rework, excess inventory and unnecessary movement.

Whistleblowing

Reporting suspected wrongdoing through a channel that protects the person reporting from retaliation.

Workflow redesign

Changing the sequence, roles and handoffs of a process — for example, to incorporate automation or AI assistance — rather than adding a new tool to an unchanged process.

Using this publication

Citation

Corporate Business Alliance (2026). Compliance & Risk Professional: CBA Standard, version 7.1.
London: Corporate Business Alliance.

Terms of use

© Corporate Business Alliance 2026. You may download, print and use this publication, and share it unaltered and free of charge, for personal study and within your organisation. It may not be sold, or republished in whole or in part, without the written permission of the Corporate Business Alliance.

Status

The CBA Standards and CBA credentials are the professional standards and certifications of the Corporate Business Alliance. CBA credentials are not regulated qualifications, and CBA is not accredited to ISO/IEC 17024; CBA claims no equivalence to the qualifications of any other body.

Publisher

Corporate Business Alliance Ltd

Registered office: 167–169 Great Portland Street, 5th Floor, London, W1W 5PF, United Kingdom
support@cba-uk.com · cba-uk.com