



Security Certification Landscape

CISSP, CISM, CISA, CRISC, CEH, OSCP and the CompTIA track | focus, audience, format, experience, career path, how to choose

[#Certifications](#) [#CareerPath](#) [#StudyPlan](#) [#Comparison](#)

Who issues what

INFO

Figures below are the ones the issuers publish (verified 2024-2026); prices, fees and minor rules change often, so check each issuer's exam page before booking. Full names: **CISSP** Certified Information Systems Security Professional; **CISM** Certified Information Security Manager; **CISA** Certified Information Systems Auditor; **CRISC** Certified in Risk and Information Systems Control; **CEH** Certified Ethical Hacker; **OSCP** OffSec Certified Professional; **CySA+** Cybersecurity Analyst; **CCSP** Certified Cloud Security Professional; **CGEIT** Certified in the Governance of Enterprise IT; **CDPSE** Certified Data Privacy Solutions Engineer.

ISC2 — Non-profit that issues CISSP, CCSP, SSCP, CC and the CISSP concentrations (ISSAP, ISSEP, ISSMP).

ISACA — Professional association for audit, governance and risk; issues CISA, CISM, CRISC, CGEIT and CDPSE.

EC-Council — Commercial training body that issues CEH, CHFI, CPENT and related certifications.

OffSec — Offensive Security, the company behind the PEN-200 course and the hands-on OSCP exam.

CompTIA — Vendor-neutral IT association; Security+, CySA+, PenTest+, SecurityX (ex-CASP+) and SecAI+.

ISO/IEC 17024 — Standard for bodies that certify persons; CISSP, CISM, CISA, CRISC, CEH and the CompTIA security exams are accredited under it (check each issuer).

DoD 8140 — US Department of Defense cyber workforce qualification framework that replaced DoD 8570; lists accepted certifications per work role.

CPE / CEU — Continuing professional education credits (ISC2, ISACA) or continuing education units (CompTIA) needed to keep a certification active.

Cert	Issuer	Focus	Audience	Level
CISSP	ISC2	Broad security programme, 8 domains	Security managers, architects, senior engineers	Senior
CISM	ISACA	Security governance and programme management	Security managers, CISO track	Senior
CISA	ISACA	IS audit, control and assurance	IT auditors, assurance, compliance	Mid-senior
CRISC	ISACA	IT risk identification, response, reporting	Risk managers, control owners	Mid-senior
CEH	EC-Council	Attack techniques and tools, knowledge exam	Early pentesters, SOC, HR-filter roles	Entry-mid

OSCP	OffSec	Hands-on exploitation and reporting	Penetration testers, red teamers	Mid
Security+	CompTIA	Security fundamentals	First security role, DoD baseline	Entry
CySA+	CompTIA	SOC analysis, detection, vulnerability management	SOC and blue-team analysts	Mid
PenTest+	CompTIA	Pentest process, scoping, reporting	Junior pentesters, vulnerability testers	Mid
SecurityX	CompTIA	Hands-on security architecture and engineering	Senior engineers, architects	Senior
SecAI+	CompTIA	Securing AI systems and using AI in security	Engineers adopting AI	Mid

Exam format and experience requirements

Cert	Items	Time	Passing	Style
CISSP	100-150 (CAT: computerized adaptive testing)	3 h	700/1000	Adaptive, no going back
CISM	150	4 h	450 (200-800 scale)	Multiple choice
CISA	150	4 h	450 (200-800 scale)	Multiple choice
CRISC	150	4 h	450 (200-800 scale)	Multiple choice
CEH v13	125	4 h	Cut score varies by form	Multiple choice; Practical is a separate 6 h lab
OSCP / OSCP+	Lab machines, 100 points	23 h 45 min + 24 h report	70 points	Proctored hands-on plus written report
Security+ SY0-701	90 max	90 min	750 (100-900)	MCQ (multiple choice) + PBQ (performance-based, simulated task)
CySA+ CS0-003	85 max	165 min	750 (100-900)	MCQ + PBQ
PenTest+ PT0-003	90 max	165 min	750 (100-900)	MCQ + PBQ
SecurityX CAS-005	90 max	165 min	Pass/fail	MCQ + PBQ
SecAI+ CY0-001	Check comptia.org	Check comptia.org	Check comptia.org	MCQ + PBQ

Cert	Experience to be certified	Maintenance
CISSP	5 years paid in 2+ of the 8 domains; 1-year waiver (degree or approved credential); Associate of ISC2 until then	120 CPE per 3 years, annual fee
CISM	5 years in information security, including 3 years in security management across the job-practice domains	120 CPE per 3 years (min 20 per year), annual fee
CISA	5 years in IS audit, control, assurance or security; waivers of up to 3 years exist	120 CPE per 3 years (min 20 per year), annual fee

CRISC	3 years in IT risk and control across at least 2 of the 4 domains (check the domain rule on isaca.org)	120 CPE per 3 years (min 20 per year), annual fee
CEH	Official training, or 2 years of security experience with an eligibility application	EC-Council ECE credits over 3 years (check current rule)
OSCP+	None enforced; PEN-200 course expected	OSCP+ valid 3 years (renew by CPE, another OffSec exam or re-exam); original OSCP does not expire
Security+	None enforced; about 2 years of IT with security recommended	50 CEUs per 3 years
CySA+	None enforced; Security+ level plus analyst experience recommended	60 CEUs per 3 years
PenTest+	None enforced; 3-4 years hands-on recommended	60 CEUs per 3 years
SecurityX	None enforced; 10 years IT including 5 years hands-on security recommended	75 CEUs per 3 years

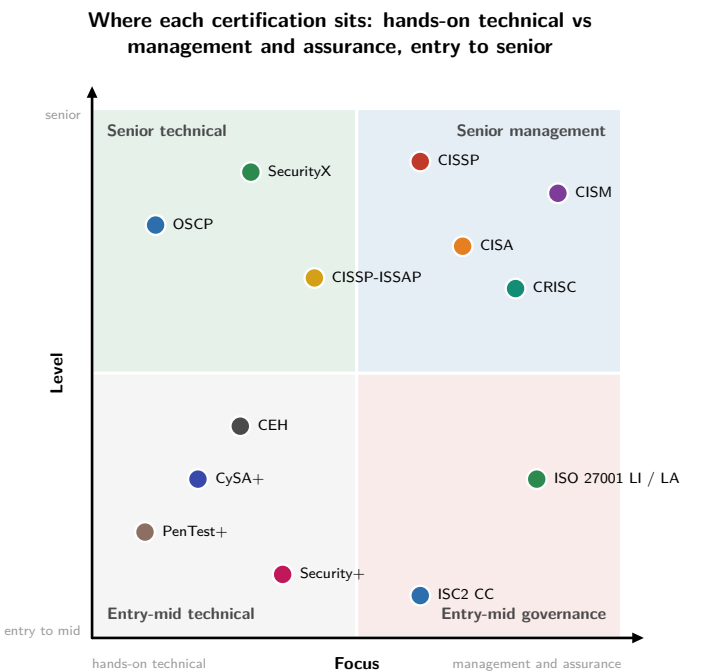
EXAM TIP

ISACA candidates may pass before they have the experience: ISACA allows the experience to be gained within 10 years before applying or up to 5 years after passing (check the current rule). ISC2's equivalent is the Associate of ISC2 status with 6 years to gain the experience.

OSCP+ (November 2024 changes)

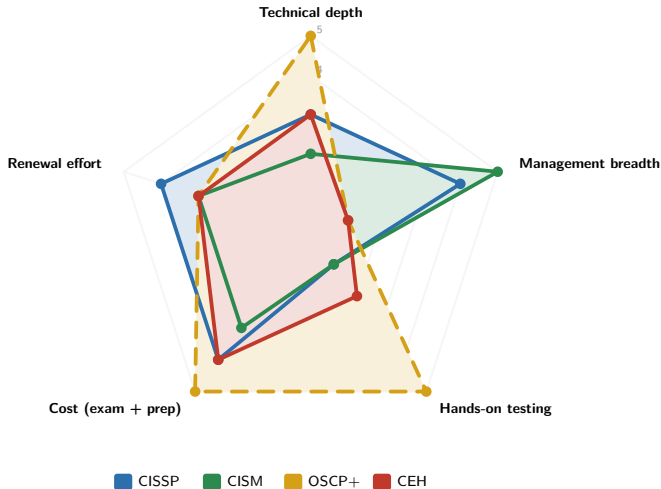
Since 1 November 2024, passing the exam grants **OSCP+**, valid three years; holders of the original OSCP keep it for life. The exam gained a mandatory Active Directory set in an assumed-breach scenario (a low-privilege domain account is given, 40 points for the whole set), kept three standalone machines (up to 60 points, 20 each) and dropped the 10 bonus points once earned from course exercises. Pass mark stays 70/100, and a professional report with reproducible steps is mandatory: without it, points do not count.

© Positioning: technical depth vs management breadth



	Governance	Risk	Audit	Architecture	Operations	Offense
CISSP	5	5	3	5	4	2
CISM	5	5	2	2	4	1
CISA	4	3	5	2	3	1
CRISC	4	5	3	2	2	1
CEH	1	1	1	2	2	5
OSCP	1	1	1	1	1	5
Security+	3	3	2	3	4	2
CySA+	1	2	1	2	5	2
PenTest+	2	2	1	1	1	5
SecurityX	3	3	2	5	4	2

Coverage by area: 5 = core, 3 = tested, 1 = marginal (editorial estimate)



Profile of four popular certifications, 0 = low, 5 = high (editorial estimate). Cost counts exam plus the usual prep (OSCP+ needs a PEN-200 lab subscription); renewal effort counts CPE (continuing professional education) hours, fees and re-testing.

Topic	CISSP	CISM	CISA	CRISC
Governance, strategy, policy	D1	D1	D2	D1
Risk assessment and analysis	D1	D2	D1 (audit risk)	D2
Risk response, KRIs, reporting	D1	D2	D2	D3

KRI = key risk indicator

Audit process, sampling, evidence	D6	—	D1	—
Controls, programme, metrics	D1, D7	D3	D2, D5	D3, D4
Asset classification, data lifecycle	D2	D3	D5	D4
Architecture, cryptography, cloud	D3	—	D5	D4
Network security	D4	—	D5	D4
Identity and access management	D5	D3	D5	D4
SDLC, acquisition, change	D8	D3	D3	D4
SDLC = software development life cycle				
Incident response	D7	D4	D4	D3
BIA, BCP, DRP	D1, D7	D4	D4	D4
business impact analysis, continuity and disaster recovery plans				
Third-party and vendor risk	D1	D3	D2	D3
Privacy	D1, D2	—	D2	D4

✓ covered ◯ partly covered ✗ not covered
Where one topic is tested in each exam: domain number (D) in the current outline; — = not a tested topic (editorial mapping, domain names listed below)

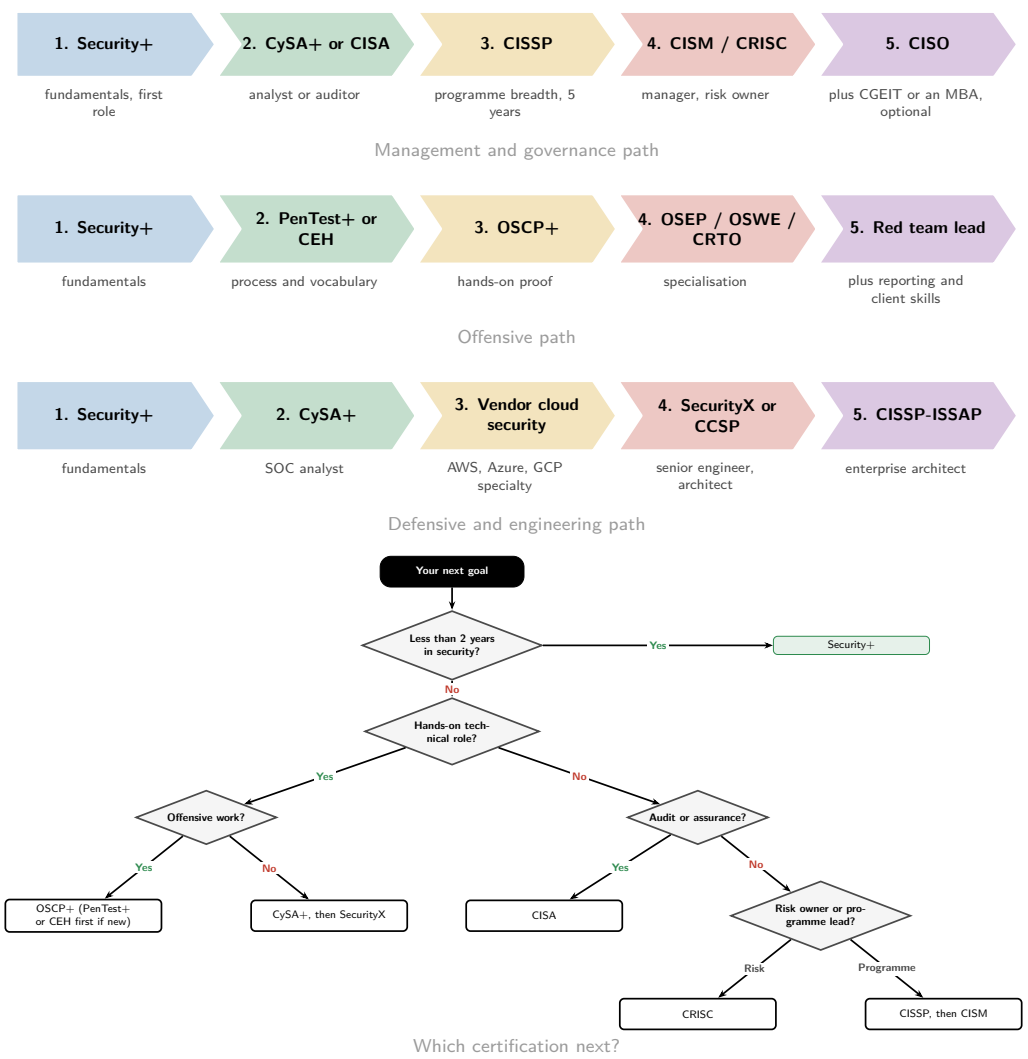
Domain names behind the crosswalk. **CISSP** (2024 outline): D1 Security and Risk Management, D2 Asset Security, D3 Security Architecture and Engineering, D4 Communication and Network Security, D5 Identity and Access Management, D6 Security Assessment and Testing, D7 Security Operations, D8 Software Development Security. **CISM** (2022): D1 Information Security Governance, D2 Information Security Risk Management, D3 Information Security Program, D4 Incident Management. **CISA** (2024): D1 Information System Auditing Process, D2 Governance and Management of IT, D3 Information Systems Acquisition, Development and Implementation, D4 Information Systems Operations and Business Resilience, D5 Protection of Information Assets. **CRISC** (2021): D1 Governance, D2 IT Risk Assessment, D3 Risk Response and Reporting, D4 Information Technology and Security. The same topic is examined through a different lens: CISA audits it, CRISC assesses its risk, CISM manages it, CISSP designs and operates it.

CISSP	CISM
Mile wide: eight technical and managerial domains	Management depth: governance, risk, programme, incidents
Credibility with engineers and managers	Credibility with executives and auditors
Adaptive exam, 3 h	Linear 150 items, 4 h

CEH vs OSCP for a pentest career

✓ CEH	✗ OSCP
+ Recognised by HR filters and some government matrices	— Proves you can compromise and report under time pressure
+ Broad vocabulary of attack classes	— Valued by pentest firms and red teams
+ No lab required for the knowledge exam	— Hard: lab time of several months is typical

Career paths



Before paying for any exam

✓ baseline / mandatory □ recommended – verify in your context

- ✓ Read the current exam outline or job practice on the issuer's site
- ✓ Confirm the experience rule and whether you can pass first and qualify later
- **MUST** Budget the annual fee and CPE effort for the whole cycle
- **SHOULD** Check which certifications your target employers and contracts ask for (DoD 8140, public tenders)

□ **COULD** Stack certifications whose CPEs overlap (one course can count for several)

- Q1 A SOC analyst with 3 years' experience wants recognition for detection work. Best fit?**
A CySA+ (analysis, detection, vulnerability management); CISSP later, once 5 years in two domains are reached.
- Q2 An IT auditor must assess controls over change management and access. Which certification matches the job?**
A CISA: IS audit process, governance, acquisition, operations and protection of assets.
- Q3 A security manager wants the most recognised broad credential for a CISO track. Which pair?**
A CISSP for breadth and credibility, then CISM for governance and programme depth.
- Q4 What changed for OSCP holders on 1 November 2024?**
A New passes grant OSCP+, valid 3 years; the exam includes an assumed-breach AD set and no bonus points. Existing OSCP stays lifetime.

How each exam thinks

The same scenario has a different right answer depending on the exam, because each certification tests a different job. Knowing the persona the exam expects is worth more points than any single fact.

Exam	Persona	Typical best answer
CISSP	Security adviser to management	Protect people first, then align with business goals; choose policy, risk assessment or process before a technical fix
CISM	Information security manager	Align with business objectives and obtain senior management support; the business owner accepts risk, not the security manager
CISA	Independent IS auditor	Gather sufficient evidence, report findings to the audit committee, never implement or fix controls yourself (independence)
CRISC	Risk practitioner	Identify and analyse risk in business terms, hand the decision to the risk owner, monitor with KRIs (key risk indicators)
CEH	Tool and technique vocabulary	Name the phase, technique or tool; pick the countermeasure that directly defeats it
OSCP	Hands-on tester	Enumerate thoroughly, gain proof, document every step so a client can reproduce it

One scenario, four answers
Scenario: an unpatched internet-facing server is discovered. **CISSP**: assess the risk and apply change management before patching. **CISM**: inform the asset owner, who decides the treatment in line with risk appetite. **CISA**: document the finding with evidence and report it; recommend, do not patch. **CRISC**: record it in the risk register, evaluate exposure against appetite, propose a response to the owner.

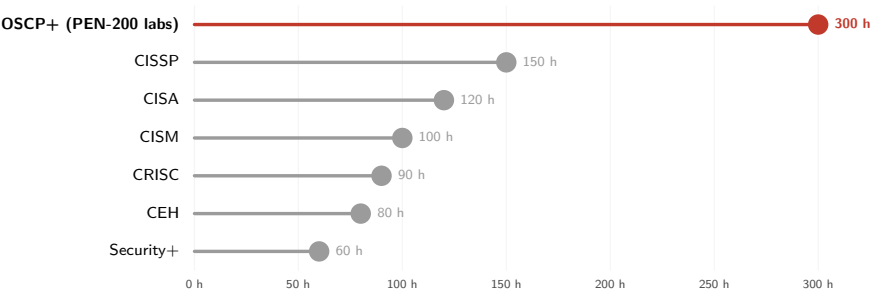
Scaled score — Raw points converted to a fixed scale so exam forms of different difficulty are comparable; ISACA 450/800 and ISC2 700/1000 are not percentages.

CAT — Computerized adaptive testing: each answer sets the difficulty of the next item and the exam stops once the candidate's ability is estimated with confidence.

Job practice — ISACA's name for the exam outline: domains, weights and task statements derived from a survey of practitioners.

Endorsement — ISC2 step after passing: a certified member attests the candidate's experience and ethics before the credential is awarded.

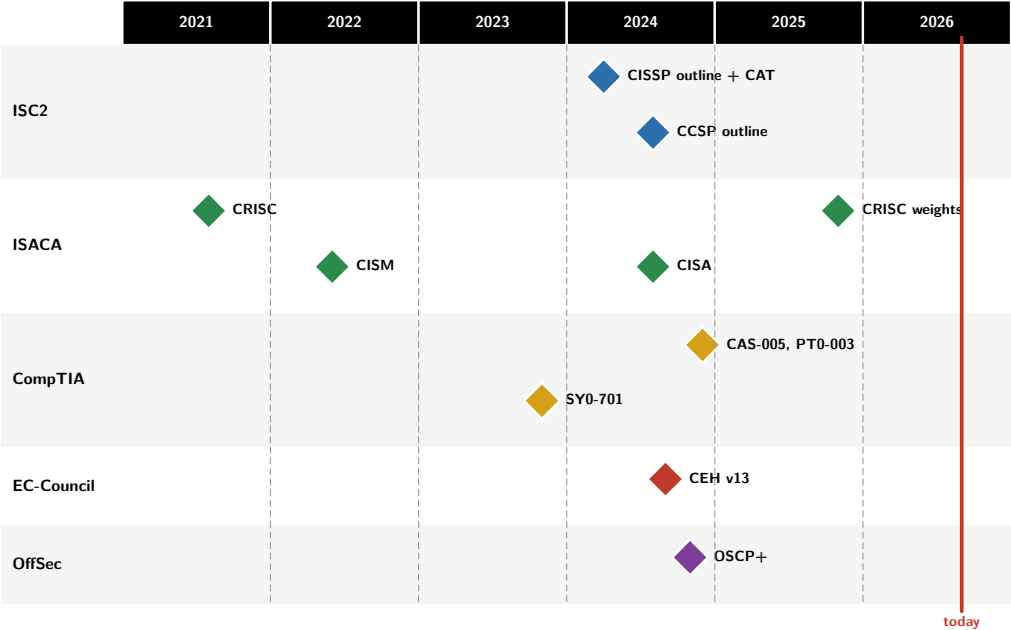
Typical self-study effort for a candidate with the required experience (editorial estimate)



- OSCP+** live exploitation plus report
 - SecurityX, CySA+, PenTest+** performance-based questions simulate tasks
 - CEH (knowledge exam)** tool recognition; CEH Practical is the hands-on part
 - CISSP, CISM, CISA, CRISC** judgment in multiple-choice scenarios
- Hands-on skill actually tested (5 = must perform the task, 1 = recognise only)

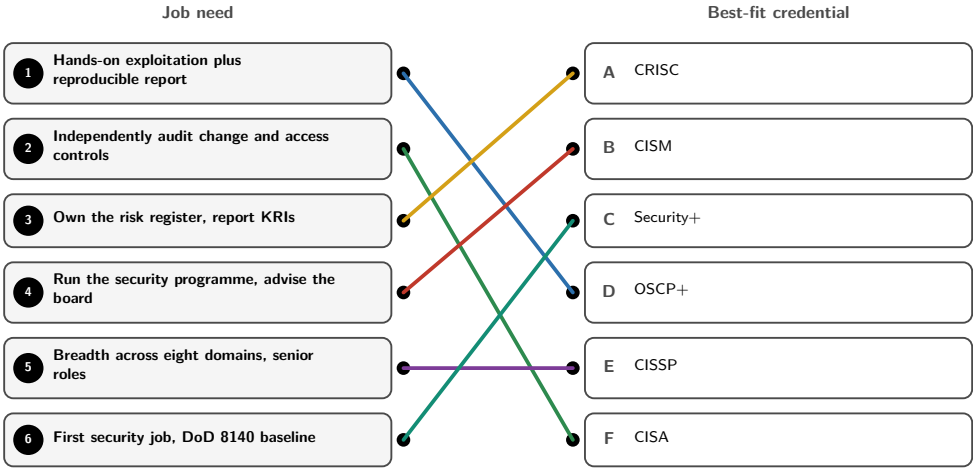
Recent changes worth knowing (2024-2026)

- CISSP outline refresh** new outline effective 15 April 2024; same 8 domains, weights adjusted
- CAT 100-150 items, 3 h** ISC2 shortened the adaptive exam in April 2024 (was 125-175 items, 4 h)
- OSCP+ with 3-year validity** renewal now required for new passes since November 2024
- CASP+ renamed SecurityX** CAS-005 launched December 2024
- DoD 8570 retired** replaced by DoD 8140 role-based qualification (verify transition dates for your contract)



Exam changes since 2021, month of first use: CISSP new outline with CAT (computerized adaptive testing) of 100-150 items in 3 h; CCSP outline refresh; new ISACA job practices (CRISC Aug 2021, reweighted Nov 2025); CompTIA Security+ SY0-701, SecurityX CAS-005 (ex-CASP+) and PenTest+ PT0-003; CEH v13 adds AI content (Sept 2024); OSCP+ valid 3 years.

Self-test: match the job need to the credential



Matching drill built from the persona table above: each exam tests a different job, so the job decides the credential