



CREST Guidance Note

Application of Accreditation Standards to Business and
Government Cyber Security Teams

Contents

1. Purpose	3
2. Scope and applicability	3
3. Core interpretation principle.....	3
4. Key definitions and interpretation	4
5. Boundary of assessment	5
6. Application to the Company General Requirements	5
Domain 1: Operating Organisation.....	6
Domain 2: Workforce Management	6
Domain 3: Quality Management and Complaint Handling	6
Domain 4: Information Security Management.....	6
Domain 5: Legal Compliance	7
Domain 6: Governance	7
7. Application to service-specific Accreditation Standards.....	7
8. Worked example: Penetration Testing	7
Domain 1: Preparation	8
Domain 2: Scoping.....	8
Domain 3: Assignment execution.....	8
Domain 4: Post-technical delivery and reporting.....	8
Domain 5: People	8
Domain 6: Technology and tools	9
9. Non-applicability and alternative evidence	9

1. Purpose

This guidance note explains how CREST Accreditation Standards should be interpreted where the applicant is a cyber security team, business unit, department or function operating within an enterprise or government organisation, rather than an external service provider.

For the purposes of this guidance, these applicants are referred to collectively as teams.

The underlying accreditation requirements remain unchanged. Teams are expected to demonstrate the same standards of professionalism, competence, governance, information security, quality management and ethical conduct as external service providers.

However, some requirements may be evidenced differently because a team may operate within a wider parent organisation and rely on shared corporate functions, internal governance arrangements and internal service delivery processes.

2. Scope and applicability

This guidance applies to Business or Government Teams seeking CREST accreditation against the Company General Requirements and one or more service-specific accreditation standards.

A team may be structured as a business unit, department, function, centre of excellence, shared service or other defined organisational capability that delivers cyber security services within a parent organisation or corporate group.

This guidance may be applied to service areas including, but not limited to:

- penetration testing;
- security operations centre services;
- cyber threat intelligence;
- incident response;
- vulnerability assessment;
- security architecture;
- incident exercising;
- other CREST-accredited services where the service is delivered internally.

This guidance does not establish a separate or lower standard. It explains how teams may demonstrate equivalent assurance against the intent of the existing accreditation requirements.

3. Core interpretation principle

Teams must demonstrate equivalent assurance against the intent of each applicable requirement.

Where a standard refers to external clients, commercial engagements, contracts or service delivery to customers, a team may provide equivalent evidence from its internal operating environment. This may include internal customers, business owners, system owners, project sponsors, risk owners, governance forums, engagement approvals, internal service records, risk acceptance processes, remediation tickets and internal reporting mechanisms.

The use of internal evidence does not reduce the level of assurance required. Internal teams must still demonstrate that services are properly governed, authorised, scoped, delivered, quality assured, reported and improved.

4. Key definitions and interpretation

Term	Guidance
Organisation	References to the “organisation” should be interpreted as the internal team, department, business unit or function seeking accreditation, together with the parent organisation and any shared corporate functions on which the team relies.
Parent organisation	The parent organisation is the legal entity or wider corporate structure within which the teams operate. Evidence relating to legal registration, financial standing, insurance, corporate policies, HR processes and organisational governance may be provided at parent organisation level where those arrangements apply to the teams.
Client	References to the “client” should be interpreted as the internal customer, stakeholder, business unit, system owner, application owner, project sponsor, risk owner, control owner or other internal recipient of the service.
Engagement	References to an “engagement” should be interpreted as an authorised internal service activity, assessment, test, investigation, review, exercise or project delivered by the internal team.
Contract, service agreement or client-facing material	References to contracts, service agreements or client-facing materials may be satisfied through equivalent internal documentation. This may include internal service descriptions, service catalogues, rules of engagement, internal statements of work, project charters, authorised test plans, governance approvals, risk acceptance records, internal reports, remediation plans or formal tickets.
Commercial insurance	Teams may not hold separate commercial insurance in the way an external provider would. Where this is the case, the applicant should demonstrate how the parent organisation identifies, manages, accepts, transfers or insures risks arising from the internal team’s activities.

	Evidence may include corporate insurance policies, self-insurance arrangements, risk acceptance records, legal indemnity arrangements, internal control frameworks or confirmation that the team's activities are covered by the parent organisation's risk management arrangements.
Complaints	Complaints may be raised as service concerns, stakeholder dissatisfaction, escalations, governance issues, audit findings, risk issues or service improvement requests. Evidence may include internal escalation routes, service management processes, issue logs, governance forums, stakeholder feedback mechanisms, audit findings, risk committee papers or formal grievance and escalation procedures.

5. Boundary of assessment

The accreditation assessment focuses on the team's capability to deliver the relevant cyber security service.

Ordinarily it should not require assessment of the entire parent organisation unless the parent organisation's controls are directly relied upon to satisfy a requirement.

The applicant should therefore clearly document:

- the team or function seeking accreditation;
- the legal entity or parent organisation within which it operates;
- the services covered by the accreditation;
- the internal customers or stakeholders served by the team;
- any central corporate functions relied upon;
- any contractors, outsourced providers, partner teams or shared services involved in delivery;
- the accountable senior owner for the accredited service.

Where shared corporate functions are used as evidence, the applicant must show that those functions apply to the team and are effective in supporting delivery of the accredited service.

6. Application to the Company General Requirements

The Company General Requirements apply to teams, but some requirements may be evidenced through the parent organisation or shared corporate functions.

Domain 1: Operating Organisation

For teams, legal registration, good standing and ultimate beneficial ownership should be evidenced at parent organisation or relevant legal entity level. The internal team should also provide an organisational chart or equivalent evidence showing its position within the parent organisation and the senior owner accountable for the accredited service.

Financial standing may be evidenced through the parent organisation's financial position, approved budgets, headcount planning, investment approvals, resource allocation or senior management commitment to maintain the service.

Commercial insurance may be evidenced through corporate insurance, self-insurance, internal risk acceptance or other arrangements that demonstrate operational risks arising from the team's activities are appropriately managed.

Domain 2: Workforce Management

Teams may rely on central HR processes for vetting, onboarding, training, competence management, offboarding and notification of significant employee changes, provided those processes apply to the team and are demonstrably followed.

The team should be able to show that individuals performing the accredited service are suitably skilled, trained, supervised and authorised for their roles. Examples may include individual and team skills, competence or training records

Where contractors, secondees, outsourced providers, partner teams or group companies are used in delivery, the internal team must demonstrate appropriate due diligence, onboarding, supervision, contractual protection, confidentiality controls and competence validation.

Domain 3: Quality Management and Complaint Handling

Teams should evidence quality management through documented service processes, peer review, management review, internal audit, stakeholder feedback, service performance monitoring, lessons learned and continuous improvement.

Complaint handling may be evidenced through internal escalation, service issue management, governance reporting, stakeholder feedback processes, audit actions or risk management routes. The process should allow concerns to be raised, reviewed, escalated where appropriate and used to improve the service.

Domain 4: Information Security Management

Teams may rely on corporate information security policies and controls where they apply to the team. The team should also demonstrate service-specific controls for protecting sensitive operational, customer, employee, technical, investigative or testing data.

Evidence may include information security policies, access control records, system hardening standards, vulnerability management records, cyber hygiene training, data handling procedures and security reviews of tools or platforms used by the team.

Domain 5: Legal Compliance

Teams should demonstrate that relevant legal and regulatory requirements are understood and applied to internal service delivery. This may include data protection, employment law, cybercrime law, financial sector regulation, sector-specific rules, monitoring and surveillance requirements, testing authorisation and cross-border data transfer obligations.

Where the standard refers to legal references in client-facing materials, internal teams may provide equivalent internal materials such as engagement documents, test authorisations, rules of engagement, service descriptions, internal reports or risk acceptance records.

Domain 6: Governance

Teams must demonstrate ethical conduct, accountability, oversight and alignment with CREST's Code of Conduct and Code of Ethics.

Community engagement may include participation in the external cyber security community and, where appropriate, internal communities of practice, internal knowledge sharing, working groups, technical forums, research, presentations, mentoring, publications or other activities that support the development of cyber security capability.

7. Application to service-specific Accreditation Standards

Service-specific accreditation standards apply equally to teams. Teams must demonstrate the same level of technical competence, control, professionalism, quality assurance and governance expected of external providers.

Where a service-specific standard refers to a client, this should be interpreted as the internal customer, business unit, system owner, risk owner, project sponsor or other internal stakeholder receiving the service. Where the standard refers to contracts, client authorisation, engagement documentation or client reporting, internal teams may provide equivalent internal evidence such as internal rules of engagement, service catalogues, authorised test plans, governance approvals, risk acceptances, change records, remediation tickets, internal reports and stakeholder sign-off.

The use of internal evidence does not lower the standard. Teams must still show that the service is properly authorised, scoped, delivered, quality assured, reported and improved.

8. Worked example: Penetration Testing

The following examples show how the interpretation principles may be applied to an internal penetration testing team.

Domain 1: Preparation

Teams must protect information before, during and after testing. Where NDAs are not used internally, equivalent controls may include employment confidentiality obligations, internal acceptable use policies, information classification schemes, privileged access agreements, project-specific access controls and internal rules of engagement.

The internal team should demonstrate data handling, encryption, segregation of sensitive information, access control, personal data protection and compliance with applicable laws in the same way as an external provider.

Domain 2: Scoping

Penetration tests must be formally scoped and authorised before testing begins. Evidence may include internal rules of engagement, approved test plans, change records, system owner sign-off, business owner approval, risk owner approval, test windows, incident escalation plans, stakeholder communication plans and records of scope deviation approvals.

Ordinarily operating as a team should not be treated as standing permission to test any system at any time. The team must be able to demonstrate that the scope, objectives, boundaries, limitations, communication routes and escalation arrangements were understood and approved by appropriate stakeholders.

Domain 3: Assignment execution

Teams are expected to meet the same technical execution requirements as external providers. It does not reduce the need for controlled techniques, safe exploitation, standardised methodology, systematic enumeration, secure testing platforms, monitoring, malware prevention, attack infrastructure protection or evidence that testing remained within scope.

Domain 4: Post-technical delivery and reporting

Reports may be issued through internal governance, risk management or remediation systems, but they must still be clear, complete, quality assured and actionable.

Evidence may include formal reports, executive summaries, technical findings, remediation tickets, risk registers, peer review records, QA sign-off records, vulnerability classification outputs and evidence that findings were communicated to relevant stakeholders.

A ticket or vulnerability record may be acceptable where it captures the required information. However, a ticket alone may not be sufficient if it does not evidence scope, methodology, risk, impact, remediation advice, quality review and completion of the engagement.

Domain 5: People

Teams must demonstrate that individuals performing penetration testing are suitably skilled, experienced and supervised. Where the internal team does not use commercial engagement roles, equivalent responsibilities should be mapped to named individuals.

For example, the team should be able to identify who performs the role of technical lead, tester, reviewer, stakeholder liaison and remediation coordinator. One person may hold more than one responsibility where this is appropriate to the size and complexity of the team or engagement.

Domain 6: Technology and tools

Teams should evidence approved tool inventories, tool review processes, internal approval for tool use, configuration standards, secure storage of outputs and processes for reviewing automated findings and applying manual testing judgement.

Where tools are provided by the parent organisation, the team should demonstrate that they are authorised, maintained, updated, fit for purpose and used in accordance with documented procedures.

9. Non-applicability and alternative evidence

Teams may identify some requirements that are not directly applicable in their commercial form, such as external client contracts or separate professional indemnity insurance. In these cases, the applicant should provide a rationale and alternative evidence showing how the intent of the requirement is met.

The applicant should not simply mark a requirement as not applicable because it uses commercial language. The correct approach is to explain how the requirement applies in the internal context and provide equivalent evidence.

Where a requirement is genuinely not applicable, the applicant should document:

- why the requirement is not applicable;
- who approved the interpretation;
- what alternative controls or evidence are in place, if any;
- whether the non-applicability affects the scope of accreditation.