ICDIP

Institute of Cyber Digital
Investigation Professionals

CONTACT US

Chartered Institute of
Information Security

ICDIP
Institute of Cyber Digital
Investigation Professionals

To apply for membership please contact the Chartered Institute of Information Security (CIISec) who run the ICDIP.

ICDIP@CIISec.org or visit our website HERE

The Institute of Cyber Digital Investigation Professionals (ICDIP) promotes, develops, and represents the professionalism, integrity and excellence of those operating within cyber digital investigations.

Our principal objectives are:

- To assure the quality and standards of cyber digital investigations for the benefit of the public
- Maintain and develop high standards of competency and skills amongst cyber digital investigation individuals across the UK
- Act as the single professional body representing those at the heart of cyber digital investigations

ICDIP was founded to professionalise Law Enforcement Agency (LEA) cyber digital investigation specialists. It now includes individuals from other organisations who undertake or support cyber digital investigations.

The Institute provides organisations with confidence that individuals who achieve accredited membership have professional recognition and status for the specialist work that they perform on a day to day basis. The process was designed following extensive consultation with stakeholders and Law Enforcement Agencies to develop a skills and standards framework that captures the essence of the cyber digital investigation profession's specialisms.

The accreditation process is an assessment of competency, involving a portfolio of evidence and interview (depending on the level applied for).

JOB FAMILIES

There are five job families (rather than individual roles) which are deemed as being at the core of a professional cyber digital investigation. These form the basis of the ICDIP skills and standards framework which is used to assess candidates.

Analyst	Forensic	Investigator	Intelligence	Interviewer
A person who gathers and critically analyses data to identify associations, trends, key factors, attributions, hypotheses, possible results and recommendations as part of an investigation.	A person who systematically extracts digital evidence for scientific analysis as part of an investigation.	A person who systematically seeks, gathers, evaluates and presents evidence as part of an investigation.	A person who systematically identifies, gathers and evaluates information to develop intelligence as part of an investigation.	A person who conducts interviews with witnesses and suspects to gather evidence and testimony as part of an investigation.

It is for the candidate to determine in which job family their skills predominantly sit.

SKILL CATEGORY AND LEVELS

Practitioner

Those who perform the practical elements involved in a cyber digital investigation. The Practitioner category predominantly draws upon the psychomotor (or 'doing') skill sets. For example, a person whose job it is to dismantle or interrogate a mobile phone to extract information.

Strategist

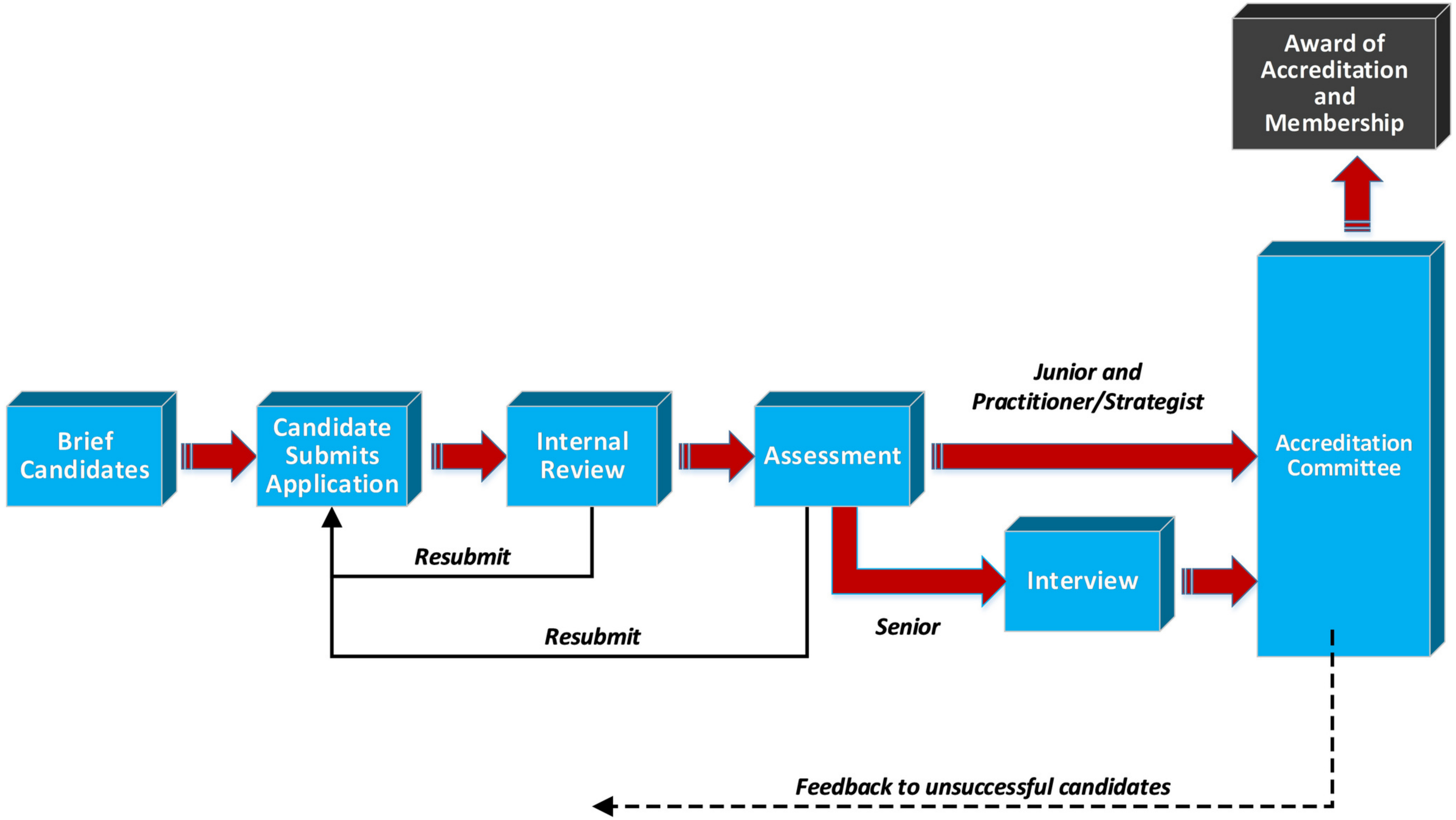
Those associated with strategist elements of a cyber digital investigation draw upon the affective skill categories. The skills for strategist's cover setting the direction, negotiating, management, coordinating and authorising processes and practices at a corporate level. For example, a person whose job it is to write the policy around how to take dismantle or interrogate a mobile phone to extract information in accordance with regulations or legislative requirements.

There are 3 levels of accredited membership for each job family which align with the skill levels.

<table>
<tr><th>Skill Levels</th><th>Analyst</th><th>Forensic</th><th>Investigator</th><th>Intelligence</th><th>Interviewer</th></tr>
<tr><td>Junior Practitioner
Junior Strategist</td><td colspan="5"><b>Affiliate Member</b>
Portfolio of evidence, competency based (1 Essential and 1 Core skill requiring 2 pieces of evidence for each)
1-year membership (expectation to apply for Associate within this period, opportunity to do CPD)</td></tr>
<tr><td>Practitioner
Strategist</td><td colspan="5"><b>Associate Member</b>
Portfolio of evidence, competency based (4 Essential and 6 Core skills requiring 2 pieces of evidence for each)
3 years membership (CPD required annually)</td></tr>
<tr><td>Senior Practitioner
Senior Strategist</td><td colspan="5"><b>Full Member</b>
Portfolio of evidence, competency based (6 Essential and 8 Core skills requiring 2 pieces of evidence for each) and interview
3 years membership (CPD required annually)</td></tr>
</table>

THE PROCESS

Once a candidate has identified their job family, skill category and level for submission of evidence, the following accreditation process then takes place.


Award of Accreditation and Membership
Brief Candidates
Candidate Submits Application
Internal Review
Assessment
Junior and Practitioner/Strategist
Accreditation Committee
Resubmit
Resubmit
Interview
Senior
Feedback to unsuccessful candidates

BENEFITS

- Professionalises cyber digital investigations
- Assesses competency of investigation skills, not just knowledge
- Inclusion in a network of cyber digital professionals
- Membership of CIISec and benefits including post-nominals to recognise professional membership
- Opportunities for Continuing Professional Development (CPD)
- Increased success at court
- Supports career development
- Aligned to Cybersecurity profession