Levy funded apprenticeships in:

- L5 Youth Justice Practitioner
- L4 Intelligence Analyst
- L4 Counter Fraud Investigator
- L4 Cyber Security Technologist
- L3 Risk / Compliance Officer

intelligencia

Empowering decision makers

Levy funded apprenticeships in:

- **Youth Justice Practitioner**
- **Intelligence**
- **Counter Fraud**
- **Risk/Compliance Officer**
- **Cyber Security Technologist**

With UK Government intention to deliver increasing volumes of apprenticeships as a viable alternative to University education, we believe that it is essential to offer a range of dynamic apprenticeships that will challenge bright young minds, more so in the Intelligence and Security sector. Equally, modern apprenticeships provide opportunities for role relevant upskilling, increasing existing workforce capability and mobility, without necessarily requiring new recruitment. Apprenticeships offer an opportunity for application of new knowledge and skills within a role specific setting, whilst developing other relevant behaviours and associated soft skills that may not usually be developed to the same level within traditional commercial programmes.

Traditional “white collar” apprenticeships often fail to offer the same level of skills development as more manual, traditional apprenticeships. We believe that these apprenticeships address this issue and develop recognition for the knowledge, skills and behaviours that are so critical to being a competent Intelligence, Counter Fraud, Risk or Security professional or to operate effectively within the Youth Justice sector.

intelligencia

Ofsted
Good
Provider

Why Choose Intelligencia Training for Levy Funded Apprenticeships

Having been involved in Intelligence Apprenticeships since their inception in 2013 we were chosen as the key education sector partner to provide support and guidance to the employer group that developed the Intelligence Analysis standard. Intelligencia Training have over 200 years of Intelligence and Risk experience that can be used to train, coach and develop confidence in applying the knowledge, skills and behaviours that are relevant to whichever sector our apprentices are seeking to add value.

- Intelligencia Training work closely with learners and employers to develop the most appropriate individual pathway.
- Pre programme scoping meetings with employer and apprentice working groups to ensure relevant and appropriate training pathways.
- Skills based exercises, analytical techniques and risk management models are specifically tailored to each sector and role that we work with.
- Hundreds of sector specific exercises to ensure maximum participation and practical involvement within our learning sessions.
- Live actors to increase communication, influence and risk management training within a safe and realistic environment.
- Excellent e-learning systems to ensure full visibility of progression and funding compliance to apprentices, employers and regulatory bodies.
- All staff are officially qualified in safeguarding, PREVENT and Mental Health First Aid.

intelligencia

Youth Justice Practitioner Apprenticeship Standard

- **Level: 5**
- **Funding: up to £17,000**

The Youth Justice Practitioner Standard was developed to provide a recognised and robust pathway for those supporting young people throughout the justice sector. It provides a broad and detailed curriculum that balances legislative knowledge, practical skills associated with engagement, relationship management and planning, as well as development of softer skills and behaviours that are essential within this niche area of employment.

At Intelligencia Training, we fully evaluate all apprentices prior to induction to programme and develop a pathway that is bespoke to each individual, being relevant to both sector and their organisation. With a huge breadth of experience, whilst working in the justice, security, intelligence and investigative sectors, our staff are well placed to deliver bespoke programmes to Youth Justice Practitioners and have value added modules within the curriculum that ensure capable and well-rounded practitioners.

The typical training period for the learners on our Youth Justice Practitioner Apprenticeship is 18-22 months and consists of classroom-based delivery sessions on either our premises or client sites as desired. We utilise technology for delivery as well as live actors and role relevant locations to enhance the learning experience.

Specific modules for study are defined within employer scoping and learner skill scan.

Modules:

Module 1: Self Awareness and Approach to Practice – Exploring individual and organisational values, ethics, bias, boundaries and Reflective Practice.

Module 2: Child First – The theoretical basis of Child First; the 4 Tenets of Child First Practice; and how this fits with HMIP expectations.

Module 3: Desistance – Desistance theories including risk and protective factors around the 3 domains of risk in Youth Justice.

Module 4: Data Protection and Information Sharing – Data Protection, Police Intelligence, Cyber Security and Multi-Agency Information Sharing Agreements.

Module 5: Assessments (7 sessions) – Relationship based practice, communication and engagement. Emotional Intelligence. Information gathering and conflict management. Brain development, trauma and ACEs. AssetPlus and Analysis. Critical thinking and defensible decision making. CSE and CCE to include County Lines and Contextual Safeguarding.

Module 6: Diversity and Disparity – Identifying diversity factors and their impact on offending behaviour, anti-racist practice and appropriate professional challenge.

Module 7: Lived experience and hearing the voice of children in youth justice – We will look at; Why should we listen to service user voice? What does it say? How can we use this to inform practice? How can we hear more from children?

Module 8: The Law and Legislation – The relationship between The Police, Court, HMIP and Children's Services Legislations; court practice utilising support from The Youth Justice Legal Centre.

Module 9: Report Writing – Purpose, structure and presentation of a range of assessment-based reports.

Module 10: Transitions – Identifying and responding to a range of transitions that children experience including accommodation, education, care status and custody.

Module 11: Intervention (3 sessions) – Risk Management including multi-agency responses (Prevent, MAPPA, IOM), reviews and safeguarding. Reflective practice and What Works? Planning including strengths-based approaches using community resources and multi-agency networks.

Module 12: Working with the secure estate – Working with STCs, SCHs, YOIs as well as working with DOLS in the community.

Module 13: Mental Health Awareness

Module 14: EPA Preparation, support and portfolio review

Knowledge, Skills and Behaviours

Knowledge

- Legislation and corresponding guidance relevant to all aspects of work in youth justice, including sentencing, risk of harm, safeguarding, children's rights and equality and diversity.
- Child and adolescent development and the full range of complex needs that can be detrimental to children's physical, emotional and mental health and wellbeing.
- The range of factors (e.g. substance misuse and adverse childhood experiences) that may lead to offending and anti-social behaviour and the methods for promoting desistance from these.
- The principles of professional judgement, including defensible decision making, how to guard against conscious or unconscious bias and how to maintain professional boundaries.
- The key components of relationship-based practice and the evidence-base for them.
- The range and purpose of assessment and planning tools relevant to working with children in the youth justice system.
- The range and type of services available for children in the youth justice age group, including adult service providers and how these work in relation to young people who are in transition to them.
- Protocol and process arrangements in working with multi-agencies, including the sharing and safeguarding of information in line with data protection law.
- The emotional and practical needs of specialist groups of young people, e.g. Looked After Children, girls, LGBTQ+, BAME.
- The practical, emotional and psychological impact of key types of life changes and transitions between services affecting children up to the age of 18.
- Barriers to children's effective engagement with youth justice interventions.
- The contextual aspects of risk (risk of what, to whom and circumstances in which risk is likely to be higher or lower).
- Their own safeguarding responsibilities and those of others within and outside of their organisation.
- The principles of effective programme design and implementation for reducing offending and reoffending.

Skills

- Communicate effectively face to face and in writing (including digitally) with children who encounter the youth justice system.
- Identify the factors that may lead to offending and anti-social behaviour and the methods for promoting desistance, and use these to plan individually tailored interventions.
- Promote the physical, emotional and mental health and wellbeing of children in the youth justice system by recognising and building on strengths, identifying need and taking action to protect children where necessary.
- Use a range of engagement skills to promote trust, including clarification of role, purpose of intervention and boundaries of authority.
- Develop relationships that are collaborative, motivating and child-centred using a range of strategies to engage young people and families (e.g. motivational interviewing, solution focussed methods, participatory practice, pro-social modelling and problem solving).
- Make effective use of assessment and planning tools designed for use in youth justice settings to inform decision making.
- Develop, implement and monitor plans which reflect risks and needs, and build on positive human and social capital to promote desistance.
- Select interventions and approaches to working with young people based on the best available evidence about their effectiveness in promoting desistance from offending.
- Broker access to sources of human and social capital appropriate to the needs of children in the youth justice system.
- Be an effective social advocate for children and their families.
- Share and safeguard information about children and their families in line with data protection law.
- Identify, assess and meet the needs of children and young people where there are safeguarding concerns.
- Reflect on practice within evidence-based frameworks in order to continuously improve outcomes for children in the youth justice system.
- Identify any barriers to children's effective engagement with youth justice interventions and take steps to remove or mitigate these.
- Actively protect the rights of children, challenge disproportionality and promote equality of opportunity.
- Keep accurate and timely records of all interactions relevant to the assessment, planning, implementation and review cycle.

Behaviours

- Show consistency and fairness and be evidence-informed in making decisions.
- Model and reward pro-social behaviours, including respect for diversity and being inclusive, and discourage inappropriate language and behaviours.
- Be optimistic and hopeful; non-blaming; open and honest; empathetic; and patient and calm in all interactions, including situations that are stressful.
- Operate in accordance with the legal, ethical and contractual requirements of youth justice work and maintain professional boundaries.
- Commit to team working and engage proactively with partner organisations and agencies to maximise the engagement of children in mainstream services and other positive activities.

Intelligence Analyst Apprenticeship Standard

- **Level: 4**
- **Funding: up to £11,000**

The Intelligence Analysis Standard was developed to replace previous frameworks in Intelligence Analysis and Intelligence Operations, providing a modern and appropriate route for intelligence professionals to develop and implement a relevant skill set.

Having been key to the development of both the Standard and End Point Assessment Strategy, Intelligencia Training are the UK's most experienced provider of vocational intelligence training.

At Intelligencia Training, we fully evaluate all learners prior to induction to programme and develop a pathway that is bespoke to each individual, being relevant to both sector and their organisation. With hundreds of sector specific analytical exercises, we are best placed to provide role specific opportunities for analysts to develop an appropriate analytical capability.

The typical training period for the learners on our Intelligence Analyst Apprenticeship is 15-18 months and consists of classroom-based delivery sessions on either our premises or client sites as desired.

Specific modules and depth of analytical training within each technique is defined by the apprentice's pre-induction skill scan.

Session Breakdown:

Intelligence Theory and Fundamentals
Intelligence cycle, source evaluation, collection planning, assumption and bias, critical thinking (3 sessions)

Applied Intelligence Analysis
Application of structured analytical techniques (up to 7 sessions)

Effective Communication of Intelligence Products
Report Writing, Verbal Briefing, Communication and Influence (2 sessions)

Network analysis

Geospatial analysis

Temporal analysis

Comparative Case analysis

Cone of Plausibility analysis

Analysis of Competing Hypothesis

Backcasting

Additional Modules Available:

- Introduction to Internet Research
- Use of Emotional Intelligence within an Intelligence Setting
- Cyber Security Awareness
- Mental Health First Aid

Learner Commitment
Between teaching sessions apprentices are provided with a range of knowledge and skills development based tasks to ensure competence and progression to End Point Assessment gateway. Intelligencia Training fully maps and record Off The Job requirements. All apprentices have access to our elearning platform for the duration of programme, providing constant communication with the training and assessment team and access to their live Individual Learning Record, providing clear and consistent visibility of targets and progression.

Knowledge, Skills and Behaviours

Knowledge

An Intelligence Analyst knows and understands:

- Legal and organisationally appropriate intelligence collection and storage methods, together with their limitations. This includes applying that knowledge to sensitive and classified materials and other openly accessible information.
- The implications for loss of sensitive material, remaining alert to the methods required to protect against physical and cyber security risks and what procedures to follow in the event of loss of such material?
- The processes involved in the collation and evaluation of organisationally relevant sources of information for use within intelligence products which will include learning to use specialist software systems.
- Organisationally relevant Intelligence Sources that are commonly used, such as Open Source, Imagery, Communications and Human.
- The Intelligence Cycle, including all processes involved in direction, collection, processing and dissemination of intelligence.
- The main factors influencing their respective organisational/ client environments, such as specific threats and key intelligence priorities, for example, tax evasion, passport fraud, people smuggling, organised criminality.
- The benefit of generating or using intelligence combined from a number of sources as opposed to a single source, considering how validity and credibility can be affected depending on the type used.
- How to use analytical development techniques to identify and produce key findings and judgements in assessments. Techniques could include, but are not limited to, pattern and trend analysis, geospatial analysis, network analysis, or others as appropriate to the organisation and its risks.
- Understand how to carry out data analysis from a numerical or factual perspective and interpret it, taking account of quantity and quality of data.
- How to identify intelligence gaps and opportunities for further analysis such as developing and maintaining an expert level knowledge or expertise to allow considered assessment through interpretation and evaluation.
- How to identify a range of relevant and credible information sources and recognise the need to collect new data when necessary from internal and external sources.
- How bias can affect judgement, and the dangers it presents if measures are not in place to mitigate this.

Skills

An Intelligence Analyst is able to:

- Engage with clients appropriately to ensure effective understanding of intelligence tasks and actively monitor ongoing intelligence requirements, engaging with all levels in an organisation, the customer and other interested parties in order to respond to demands.
- Recommend what information should be collected based upon identified intelligence gaps, and/or issue requests for information to external organisations to collect or process information.
- Identify, review, and interpret significant information, applying organisationally appropriate analytical techniques such as the use of diagnostics (links, patterns, and trends), scenario generation and validating assessments to identify key findings and opportunities for further analysis.
- Think critically, through objective analysis and evaluation of an issue, to form a judgement which is unbiased, undistorted and can withstand challenge.
- Produce written reports to a high standard as well as confident verbal briefings and presentation of findings, using an appropriate range of methods dependent on factors like audience, available time and the organisation's culture.
- Obtain client views on outcomes so as to feed back into the Intelligence Cycle and enrich the process of collection, processing, dissemination.
- Use existing and emerging IT (including digital) applications in the analysis, development and dissemination of intelligence products in line with organisational requirements.
- Operate in accordance with applicable security and legislative responsibilities such as applying appropriate audit trails, handling instructions, and protective markings, including the Official Secrets' Act.
- Organise appropriate disposal when working with sensitive materials.

Behaviours

An Intelligence Analyst should be:

- Confident in their ability and have courage of their convictions.
- Logical with a good attention to detail.
- Discreet and trustworthy when working with highly confidential materials.
- Open minded, innovative and a problem solver.
- Agile, able to adjust rapidly and decisively, especially when operating in complex situations.
- Persistent and resilient; not all intelligence activity will immediately be successful.
- Flexible and understand that there is more than one way of working.

Post completion qualification opportunity

Whilst there are no regulated qualifications included within this standard, upon successful completion of the apprenticeship and End Point Assessment there is an opportunity for work produced in your role whilst on programme to be mapped against the criteria for recognised professional qualifications. Work may be assessed against the criteria for the well regarded L4 Diploma in Intelligence Operations, the most popular OFQUAL regulated qualification that recognises an analyst's competence . Please note that assessment and certification are not included within the apprenticeship standard and can not be funded via The Apprenticeship Levy, as such additional commercial charges will apply.

Counter Fraud Investigator Apprenticeship Standard

- **Duration: 18-24 months dependent upon pathway chosen**
- **Funding: up to £15,000**

The Fraud Investigation Standard was developed to provide a recognised and robust pathway for fraud investigators that would allow for parity across sectors and comprehensive development of all knowledge, skills and behaviours associated with being an effective and competent investigation professional.

At Intelligencia Training, we fully evaluate all apprentices prior to induction to programme and develop a pathway that is bespoke to each individual, being relevant to both sector and their organisation. With a huge breadth of fraud, analytics and investigative experience within our staff we are well placed to deliver bespoke programmes to Fraud Investigators working across a variety of Public Sector, Law Enforcement and Financial Services roles.

The typical training period for the learners on our Fraud Investigation Apprenticeship is 18-24 months and consists of classroom/outdoor based delivery sessions on either our premises or client sites as desired.

Specific modules for study are defined within employer scoping and learner skill scan.

Modules Available:

Module 1
Fraud Principles & Methodology (1 day)

Module 2
Key Duties Of A Fraud Investigator (1 day)

Module 3
Emotional Intelligence (1 day)

Module 4
Key Legislation Relating To A Fraud Investigation (1 day)

Module 5 – Mapping A Fraud Investigation (1 day)

Module 6
Fraud Investigation Key Principles (3 days)

Module 7
Principles Of An Interview (3 days)

Module 8
Fraud Report Construction & Submission (1 day)

Module 9
The Rules Of Disclosure In A Civil Or Criminal Investigation (1 day)

Module 10
Presenting Evidence At Trials, Hearings & Tribunals (2 days)

Module 11
Supplementary Legislation Relating To A Fraud Investigation (1 day)

Module 12
The Role Of Intelligence In A Fraud Investigation (3 days)

Module 13
Open Source For Internet Based Research & Investigation

Module 14
Mental Health Awareness (1 day)

Mock End Point Assessment

Learner Commitment

Between teaching sessions apprentices are provided with a range of knowledge and skills development based tasks to ensure competence and progression to End Point Assessment gateway. Intelligencia Training fully maps and record Off The Job requirements. All apprentices have access to our elearning platform for the duration of programme, providing constant communication with the training and assessment team and access to their live Individual Learning Record, providing clear and consistent visibility of targets and progression.

Post completion qualification opportunity

Whilst there are no regulated qualifications included within this standard, upon successful completion of the apprenticeship and End Point Assessment there is an opportunity for work produced in your role whilst on programme to be mapped against the criteria for recognised professional qualifications. Work may be assessed against the criteria for the new L4 Certificate in Fraud Investigation, the first OFQUAL regulated qualification to recognise Fraud Investigation. Please note that assessment and certification are not included within the apprenticeship standard and can not be funded via The Apprenticeship Levy, as such additional commercial charges will apply.

Knowledge, Skills and Behaviours

Knowledge

- Understand the legislation and associated codes of practice relevant to investigations as well as an understanding of departmental policy. Covering appropriate laws including Police and Criminal Evidence Act 1984 (PACE), Criminal Procedure and Investigations Act 1996 (CPIA), Human Rights Act (HRA), and Proceeds of Crime Act 2002 (POCA), Data Protection legislation, Public Interest Disclosure Act 1998 (PIDA), Whistleblowing (WB) policies and equivalent Civil legislation such as the Finance Act (FA) where appropriate.
- Understand the points to prove in pursuing an investigation such as guilty mind, guilty act, and prima facie evidence.
- Develop professional knowledge of relevant legislation and regulatory requirements for the different types of investigation. Keep this knowledge up to date by identifying sources of information and identifying policy and law change.
- Understand how to open and maintain a case file and how to plan an investigation to the required standard for criminal, civil, regulatory or disciplinary investigations. Understand the Fraud Investigation Model (Criminal) / or organisational equivalent when responding to allegations of fraud.
- Understand the different types of evidence (direct, circumstantial, hearsay etc.)
- Understand the types of forensic opportunity available and when they can be used to gather evidence.
- Understand the principles of RIPA codes of practice.
- Understand why the recording of notes of interviews, conversations, evidential observations and decisions made during the course of an investigation is necessary and has knowledge of best practice use. Understand how to produce witness statements / affidavits to the standard required for all types of investigations.
- Understand why recording investigation activities / enquiries during the course of an investigation are necessary and has knowledge of best practice use. Understand the rules and relevant policies relating to the continuity of evidence such that the source of evidence can be fully supported. Understand the National Intelligence Model, National Intelligence methodology (criminal investigation) and the demarcation of intelligence and evidence and demonstrate awareness of source and evidence handling.
- Understand the relevant legislation and procedures (including Legal Professional Privilege) in the participation of a search of a person, premises, vehicles or workplaces.
- Understand how to assess the strength of evidence and the requirement to lawfully gather evidence to required standards in a criminal, civil, regulatory or disciplinary investigations, subject to role.
- Understand how to produce witness statements to the standards required by the CPIA 1996 (criminal investigations). Understand how to produce witness statements / affidavits to the standard required for non-criminal investigations.
- Understand how data may be analysed and collated to support investigative decisions and outcomes in criminal, civil, regulatory or disciplinary investigations as appropriate. Understand when the government protective marking scheme and source management processes should apply when disseminating material.
- Understand the briefing and de-briefing format.
- Understand the PEACE model and the use of conversation management and open recall techniques, how to produce an overarching investigative interviewing strategy, an interview plan and how to evaluate an investigatory interview to identify further investigative actions, to the required standard, civil, disciplinary, regulatory or criminal. Where appropriate.
- Understand the requirements for conducting an Interview Under Caution (IUC) fully compliant with the requirements of PACE and Criminal Justice Act 2003 (CJA) (criminal investigations). Understand the requirements for conducting an interview which is fully compliant with relevant legislation or departmental policy (non-criminal investigations).
- Understand the varying demands of the witness and how to respond to them.
- Understand how to produce investigator notes, narrative statements, 3rd party witness testimonies and transcripts, and the requirements for retention.
- Understand how to produce concise, timely, clear, balanced & accurate reports, briefings, letters, e-mails & other items of correspondence.
- Understand how to prepare files, applications and orders for court to the required standard for the activity undertaken.
- Understand the procedures and requirement to give evidence as a witness at hearings. (Criminal / Civil / Regulatory / Disciplinary investigations). Understand the process for referring a case to other law enforcement agencies.
- Understand compliance with the provisions for disclosure in court, tribunal or disciplinary proceedings as appropriate.
- Understand how to obtain, record & present evidence in court during proceedings.
- Understand how to provide insight from investigations to identify and facilitate improvements to policy and processes to assist prevention, deterrence and increased future detection.
- Understand how to prepare an evidence file with material to support court, tribunal or disciplinary proceedings in accordance with the requirements of the relevant legislation, codes of practice or departmental policy.
- Understand how to prepare files and investigate to the relevant standard in parallel, including the differences and associated risks in parallel investigations and the relevant parallel civil enforcement and / or recovery / compensation actions and how to progress them.
- Understand who the partners are in the counter fraud community and law enforcement sector and the need to build and maintain new and existing partner / stakeholder

relationships with those involved in investigations to achieve progress on objectives, key initiatives and shared interests.

- Understand the different types of fraud committed and how these frauds could be perpetrated, the processes required to determine the losses and costs figures in sanction and redress outcomes and how to report the outcome with recommendations.

Skills

- Apply legislation and associated codes of practice and can determine points to prove in pursuing an investigation. Apply departmental policy.
- Investigate the points to prove in pursuing an investigation.
- Identify sources of information e.g. regarding the process of policy and law change.
- Maintain case files and produce investigation plans to the required standards for criminal, civil, regulatory or disciplinary investigations. Apply the Fraud Investigation Model (Criminal) / or organisational equivalent when responding to allegations of fraud.
- Differentiate between types of evidence (direct, circumstantial, hearsay etc.) and relate their significance.
- Utilise forensic opportunities and how to apply them in investigations (where relevant to the type of investigations undertaken).
- Apply consideration of the principles of RIPA codes of practice.
- Implement best practice for note taking during the course of an investigation (where relevant to the type of investigations undertaken). Implement best practice for witness statements during the course of an investigation (Relevant to the type of investigations undertaken).
- Produce records of the investigation activities / enquires during the course of an investigation. Apply the rules and relevant policies relating to the continuity of evidence so the source of evidence can be fully supported. Apply the classification and handling of information in line with the National Intelligence Model and national intelligence methodology (criminal investigation) and appropriate handling principles to source and intelligence material, demonstrating knowledge of potential risks of mishandling.
- Participate in searches (including consideration of Legal Professional Privilege) of a person, premises, vehicles or workplaces, adhering to policy and legislation of organisation.
- Assess the strength of evidence and apply the relevant legislation and codes of practice to gather evidence to required standards, subject to role
- Produce witness statements to the required standard for the investigations e.g. Criminal Investigation Standard.
- Use analysis techniques on a range of data and make sound and fair investigation decisions in investigation as appropriate. Apply the organisation's protective marking scheme and source management before disseminating material.
- Apply the briefing and de-briefing method, disseminating information gathered to the appropriate individuals, groups, or departments as required, for all investigations.
- Utilise the PEACE model for interviewing, applying conversation management and open recall techniques, complete an overarching investigative interviewing strategy, produce interview plans, summarise and evaluate interviews to the required standard.
- Undertake an interview appropriate to the investigation being undertaken, introducing testimony and exhibits during interviews as appropriate.
- Recognise and respond to the varying demands of the witness.
- Produce and retain accurate investigator notes, narrative statements, 3rd party witness testimonies and transcripts.
- Produce concise, timely, clear, balanced & accurate reports, briefings, letters, e-mails & other items of correspondence.
- Prepare files, applications and orders for court to the required standard for the activity undertaken.
- Present evidence as a witness at appropriate hearings. Refer appropriate cases to other law enforcement agencies.
- Comply with the provisions of disclosure in legal proceedings.
- Obtain, record & present evidence in court during proceedings.
- Produce full and accurate post investigation assessments.
- Produce an evidence file with material to support court, tribunal or disciplinary proceedings in accordance with the requirements of the relevant legislation, codes of practice or departmental policy.
- Utilise the correct powers appropriate to the type of investigation.
- Build and maintain new and existing partner / stakeholder relationships to achieve progress on objectives, key initiatives and shared interests and developing beneficial working relationships.
- Categorising fraud and provide insight into how the fraud was perpetrated, calculate the losses and costs borne in cases of fraud for use in sanctions and redress outcomes.

Behaviors

- Committed, conscientious and organised even when completing multiple tasks.
- Take accountability for decisions made and for maintaining own knowledge and skills.
- Work with integrity, impartiality and excellence in line with requirements of the business and their profession.
- Inquisitive, open-minded and objective, will seek out evolving and innovative ways to add value
- Show courage, resilience and flexibility when interacting with others to ensure the best outcome.
- Work collaboratively with stakeholders to achieve common goals and have an awareness of different styles of working to ensure mutual respect.

Risk/Compliance Officer Apprenticeship Standard

- **Level: 3**
- **Funding: up to £9,000**

The Risk/Compliance Officer Standard was developed to provide a robust and recognised apprenticeship pathway for those risk and compliance professionals working across the breadth of the Financial Services sector.

At Intelligencia Training, we fully evaluate all apprentices prior to induction to programme and develop a pathway that is bespoke to each individual, being relevant to both sector and their organisation. With a huge breadth of risk experience on our staff, covering Regulatory Compliance, Financial Services, Financial Crime and Cyber Security, Intelligencia Training are able to offer a bespoke and relevant compliance/risk pathway that are very specific to individual apprentices role.

The typical training period for the learners on our Risk/ Compliance Officer Apprenticeship is 15 months and consists of classroom based delivery sessions on either our premises or client sites as desired.

Specific modules and risk/compliance pathways for study are defined within employer scoping and learner skill scan.

Session Breakdown:

- Session 1 – Risk Management Purpose, Overview, Principles and Terminology
- Session 2/3 – Compliance Frameworks, Policy and Processes, Sanctions and Penalties
- Session 4 – Organisational Objectives, Values and Purpose within a Compliance Environment
- Session 5 – Effective Communication
- Session 6/7 – Risk Analysis – Structured Analytical Techniques
- Session 8 – Assumption, Bias and Critical Thinking within Risk and Compliance
- Session 9 – Live Exercise Session (Scoped with employer to develop an actor led exercise to focus on implementation of learning within a live, safe learning environment.
- Session 10/11 – Professional Qualification preparation and exam
- Session 12 – Mock EPA

Additional Modules Available:
Understanding the Disclosure of Information
Cyber Security Awareness
Mental Health First Aid

Professional Certification

Prior to reaching End Point Assessment Gateway, all Apprentices must achieve one of the below professional certifications that are most relevant to their role and pathway, to be determined by the employer prior to programme start.

International Compliance Association:
Certificate in Financial Crime Prevention, Certificate in Compliance, Certificate in Anti-money Laundering

Chartered Institute for Security & Investment:
Combating Financial Crime, Global Financial Compliance, Risk in Financial Services, Managing Cyber Security

Learner Commitment

Between teaching sessions learners are provided with a range of knowledge and skills development tasks to ensure competence and progression to End Point Assessment gateway. Intelligencia Training fully maps and record Off the Job requirements. All apprentices have access to our elearning platform for the duration of programme, providing constant communication with the training and assessment team and access to their live Individual Learning Record, providing clear and consistent visibility of targets and progression.

Requirements:

Core Knowledge, Skills and Behaviours

Knowledge	What is required
Risk and Compliance Framework	Broad understanding of the Financial Services legal and regulatory framework, the role of the different regulators (if appropriate), the implications of non-compliance for the organisation.
Risk and Compliance policies / procedures	Sound understanding of the specific risk/compliance requirements for their role e.g.. operational risk, financial crime, know your customer, training & competence, approved persons, conduct risk, complaints, data security. This should include both the actual legal/regulatory requirements eg Financial Conduct Authority (FCA) Handbook and the policies/procedures used by the organisation to implement these requirements.
Industry and company understanding	Understands the role their organisation plays in Financial Services, the business they work in, the products and services offered to customers, the organisation's approach to delivering fair customer outcomes, its 'Values', professional standards, and where their role fits in the business. Understands the function of the different areas of the organisation they need to work with in their role. Basic understanding of the impact the external environment has on Financial Services and relevant best practice.
Systems and Processes	Understands the systems, tools and processes used in the role, together with the standards to be met, including IT tools.

Skills	What is required
Delivering Services	Uses a wide range of company systems and processes to deliver services to customers/colleagues. This may include advice to customers/colleagues based on regulatory requirements and organisation policies; working with suppliers on data security; internal reviews / audits and follow up; ensuring accurate records e.g. approved persons; supporting formal committees. Proactively meets challenging individual and team performance measures in line with company policy, Values, standards and regulatory requirements. Plans and organises their work, focusing on priorities, to meet commitments / KPIs, including regulator deadlines. Escalates when required.
Analysis and Problem solving	Analyses relatively straightforward risk/compliance problems, investigating issues e.g. fraudulent transactions, and recommending solutions. Works with data, analysing and producing required reports / management information for internal and/or external e.g. FCA use. Able to read and interpret reports, summarising required information.
Communicating & Influencing	Writes clear and concise reports / recommendations in a way that is meaningful to the recipient. Deals effectively with customers/colleagues, using sound interpersonal skills and communicating well through a range of media using appropriate language e.g. phone, face to face, email. Listens actively to understand needs and adapts their style to the recipient. Influences others to ensure compliance/risk requirements are met, when appropriate.
Teamwork	Builds/maintains strong working relationships with customers/colleagues/suppliers as appropriate. Consistently supports colleagues at all levels and collaborates to achieve results. Aware of own role in the team and impact on others.
Continuous improvement	Identifies opportunities to improve performance and service delivered. Takes ownership of specific changes that impact their role.
Personal Development	Keeps up to date with relevant legal/regulatory changes. Seeks feedback and acts on it to improve their performance. Builds their own capability through ownership of their own development, working with their manager.

Behaviours	What is required
Honesty & Integrity	Truthful, sincere and trustworthy in their actions. Shows integrity by doing the right thing. Maintains appropriate confidentiality at all times.
Flexibility	Adapts positively to changing work priorities and patterns when new tasks need to be done or requirements change.
Resilience	Displays energy and enthusiasm in the way they go about their role, dealing positively with setbacks when they occur. Stays positive under pressure.

Cyber Security Technologist Apprenticeship Standard

- **Level: 4**
- **Funding: up to £18,000**

As the UK's leading provider of Higher apprenticeships across the Protective Services sector, Intelligencia Training is at the forefront of capacity building within the intelligence, investigative and security sectors. This experience, combined with our Globally recognised and award-winning Cyber Stars Initiative, delivered worldwide to over 300,000 students, has allowed us to be pivotal to capacity building across Government agencies, the law enforcement community, banking, insurance, utilities providers and those tasked with protecting critical national infrastructure.

We are therefore delighted to be approved for delivery of the revised Level 4 Cyber Security Technologist Apprenticeship Standard and feel our experience and understanding of organisational requirements within our community make us a leading provider for this standard.

Cyber Security Technologists all require an understanding of security concepts and technology and how to mitigate risks arising from threats. The specific tasks undertaken vary depending on what needs to be achieved by the team at any particular time. Some tasks may be very technical, others may be more analytical, business or user focused. All roles in this occupation work to achieve required cyber security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil an organisations requirement.

Delivery Model:

We have developed an engaging delivery model that can follow 2 specific pathways.

1. The Cyber Risk Analyst that Focuses on risk assessment, analysis and giving advice on risk mitigations. The roles may support formal security governance, regulatory & compliance (GRC).

2. The Cyber Defender & Responder is more operationally focused, configuring and operating secure systems to prevent security breaches or monitoring systems to detect and respond to security breaches.

A brief breakdown of the learning outcomes and modules included in these pathways is featured below (Relevant content, tools and applications are customisable based on employer needs). To request a full breakdown of the Level 4 Cyber Security Technologist Apprenticeship Standard, please contact **info@intelligenciatraining.com.**

Pathway 1 | Cyber Risk Analyst

On completion of the apprenticeship the delegate will be competent to:

- Identify cyber vulnerabilities in a system to ensure security is maintained.
- Identify security threats and hazards to a system, service or processes to inform risk assessments and design of security features.
- Research and investigate attack techniques and recommend ways to defend against them.
- Support cyber security risk assessments, cyber security audits and cyber security incident management.
- Develop security designs with design justification to meet the defined cyber security parameters.
- Configure, deploy and use computer, digital network and cyber security technology.
- Develop program code or scripts for a computer or other digital technology for example an industrial control system.
- Write reports, give verbal reports and presentations in the context of the cyber security role.
- Manage cyber security operations processes in accordance with organisational policies and standards and business requirements.
- Participate in cyber war gaming and simulations (technical & non-technical), for example to better understand cyber-attack and defence, rehearse responses, test and evaluate cyber security techniques.
- Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.

- Analyse security requirements and develop a security case taking account of all applicable laws and regulations.
- Conduct cyber security risk assessments.
- Conduct cyber security audits.
- Develop information security policies to achieve security outcomes within a defined scope.
- Design and implement security awareness campaigns.

This is achieved through the completion of 11 modules over the course totalling 20 months:

- **Module 01** - Legislation, Regulation and Standards
- **Module 02** - Operating Systems
- **Module 03** - Networking Principles
- **Module 04** - Tool Development
- **Module 05** - Offensive Operations
- **Module 06** – Risk Analysis and Awareness
- **Module 07** - Governance, Risk Management and Compliance
- **Module 08** - Cryptographic Principles
- **Module 09** - Security Architectures
- **Module 10** - Threat Management
- **Module 11** - Incident Response

Pathway 2 | Cyber Defender & Responder

On completion of the apprenticeship the delegate will be competent to:

- Identify cyber vulnerabilities in a system to ensure security is maintained.
- Identify security threats and hazards to a system, service or processes to inform risk assessments and design of security features.
- Research and investigate attack techniques and recommend ways to defend against them.
- Support cyber security risk assessments, cyber security audits and cyber security incident management.
- Develop security designs with design justification to meet the defined cyber security parameters.
- Configure, deploy and use computer, digital network and cyber security technology.
- Develop program code or scripts for a computer or other digital technology for example an industrial control system.
- Write reports, give verbal reports and presentations in the context of the cyber security role.
- Manage cyber security operations processes in accordance with organisational policies and standards and business requirements.
- Participate in cyber war gaming and simulations (technical & non-technical), for example to better understand cyber-attack and defence, rehearse responses, test and evaluate cyber security techniques.
- Keep up to date with industry trends and developments to enhance relevant skills and take responsibility for own professional development.
- Manage local response to non-major cyber security incidents.
- Monitor technology systems (for example computer networks and computer systems) in real time to detect cyber security incidents, breaches and intrusions.
- Integrate and correlate information from a variety of sources and form an informed judgement on whether an indicator constitutes a likely security incident, breach or intrusion.
- Respond to a suspected security incident, breach or intrusion in accordance with organisation procedures any defined service level agreements or performance targets.
- Prevent security breaches using a variety of tools techniques and processes.

This is achieved through the completion of 11 modules over the course totalling 20 months:

- **Module 01** - Legislation, Regulation and Standards
- **Module 02** - Operating Systems
- **Module 03** - Networking Principles
- **Module 04** - Tool Development
- **Module 05** - Offensive Operations
- **Module 06** - Defensive Operations
- **Module 07** - Governance, Risk Management and Compliance
- **Module 08** - Cryptographic Principles
- **Module 09** - Security Architectures
- **Module 10** - Threat Management
- **Module 11** - Incident Response

Employer & Apprentice Commitment

Between teaching sessions apprentices are provided with a range of knowledge and skills development-based tasks to ensure competence and progression to End Point Assessment gateway. Intelligencia Training fully maps and record Off The Job requirements. All apprentices have access to our e-learning platform for the duration of programme, providing constant communication with the training and assessment team and access to their live Individual Learning Record, providing clear and consistent visibility of targets and progression.


FEWEEK aelp
APPRENTICESHIP AWARDS 2022
WINNER
PROTECTIVE SERVICES APPRENTICESHIP PROVIDER OF THE YEAR


intelligencia
FEWEEK aelp
APPRENTICESHIP AWARDS 2022
Part of the
Protective Services Apprenticeship Provider of the Year
CONGRATULATIONS TO
Intelligencia Training Limited

Intelligencia Training is the leading specialist apprenticeship provider in the UK for Intelligence Analyst, Counter Fraud Investigator, Risk and Security professionals.

intelligencia

Phone: 01234 381660

Email: info@intelligenciatraining.com

Intelligencia Training Limited
3 Appley Court
Haynes
Bedfordshire
MK45 3QQ

www.intelligenciatraining.com