Levy funded apprenticeships in:

- ▶ **L4 Intelligence Analyst**
- ▶ **L4 Counter Fraud Investigator**
- ▶ **L4 Data Analyst**
- ▶ **L3 Data Technician**
- ▶ **L3 Security First Line Manager**
- ▶ **L3 Risk / Compliance Officer**

intelligencia

Levy funded apprenticeships in:

- ▸ **Intelligence**
- ▸ **Counter Fraud**
- ▸ **Data Analyst / Technician**
- ▸ **Risk/Compliance Officer**
- ▸ **Security First Line Management**

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, Data or Risk or Security professional.

intelligencia

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, data 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

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:

- Internet Research and Investigation
- Understanding the Disclosure of Information
- 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.

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 – Counter Fraud Overview (2 days)
• Cross sector terms and definitions
• Fraud Types and associated offences
• Understanding your organisation and role
• Overarching legislation

Module 2 – Case Initiation (1 day)
• Fraud investigation model (and equivalents)
• Initiation of an investigation
• Understanding of Disclosure requirements
• Investigative Outputs
• PACE

Module 3 - Interviewing Theory (1 day)
• Assumption and bias – impact and effects
• Human Aspect – theory and behaviours
• Interview Planning
• PEACE model

Module 4 – Interviewing Witnesses/Victims (Theory and Practical Sessions – 2 days)
• Soft skills associated with interview techniques – victims/witnesses
• Evidence gathering from witness/victim
• Statements
• Conducting different types of interviews
• Special measures
• Subject matter experts and expert witnesses
• Associated legislation

Module 5 – Evidence Gathering (Physical and Digital) (3 days)
• Evidence Types and Forensic Opportunities
• Powers and Audit
• Evidence Gathering Process
• Legal Considerations
• Search Practical

Module 6 – Interviewing Offenders (2 days)
• Soft skills associated with interview technique – offenders
• Evidence gathering from Offender
• Statements
• Legal considerations
• Practical

Module 7 – Analytical Techniques to support Fraud Investigations (2 - 4 days)
• Pattern and Trend Analysis
• Comparative Case Analysis
• Network Analysis

Module 8 – Case Building (2 days)
• Definition in relation to different case/investigation types
• Disclosure – practical application
• Pathways (civil, criminal)
• Productions Orders and required outputs
• Actions to take
• Legal requirements

Module 9 – Presenting Evidence in Court (2 days)
• Theory – Court processes and procedures
• Practical – courtroom (use of actors, guest speakers, participation, defence and prosecution)

Module 10 - Planning/problem solving/team building
• Required development and evidence of role associated behaviours

Optional additional modules:
• 1 day – Internet Research and Investigation (techniques, digital footprints, due diligence)
• 1 day – Cyber Safety (human behaviours)
• 1 day – Mental Health First Aid

Mock End Point Assessment - 1 day

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

- 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.

Data Analyst Apprenticeship Standard

▶ **Level: 4**
▶ **Funding: up to £15,000**

This apprenticeship has been included into our portfolio of specialist programmes as we recognise the significant differences between intelligence and data analysis as well as the departments and roles that utilise these skills and techniques.

The ability to collect, organise and study data is a vital skill set within the vast range of public and private sectors in which Intelligencia Training operates. Building upon the growing success of our engagement via our intelligence analyst apprenticeship we are very aware of how both intelligence and data led can influence decision making processes. The Data Analyst Apprenticeship Standard focusses upon how data is collected, organised and studied to provide business insight. Data analysts are typically involved with managing, cleansing, abstracting and aggregating data, and conducting a range of analytical studies on that data. They work across a variety of projects, providing technical data solutions to a range of stakeholders/customers issues. They document and report the results of data analysis activities making recommendations to improve business performance. They have a good understanding of data structures, database systems and procedures and the range of analytical tools used to undertake a range of different types of analyses. Our engaging delivery model and highly experienced tutors with extensive multi-sector experience will deliver significant new skills.

Modules Available:

Module 1/2 –Data concepts, principles and evaluation of the date life cycle.
Key terminology Understanding data types, formats, architecture and frameworks

Module 3 – Legislation and data management
Understanding core legislation, how to legally access, process, format and utilise data from a range of sources

Module 4-5 - Data Sources and acquisition
Understanding the breadth of data sources available at various levels of the internet, how to safely and legally access, process and use this data within a corporate environment.

Module 6 - Managing Risks in Data
How to identify, evaluate and mitigate risks within data analysis roles

Module 7-14 – Applied Data phase
Familiarisation with a range of role and sector relevant data processing and analysis tools to collate, format and analyse a range of data types for descriptive, predictive and prescriptive outputs using a range of common data analysis techniques. Programmes are specific to role but include Oracle, SQL, ARC, PowerBI, Bold BI, Tableau, SAP Analytics

Module 15 – Analysis of data from multiple sources
Utilising skills developed in the Applied Data phase to collate and analyse data from multiple sources to better support decision making

Module 16 – Customer Insight and Effective Communication
Understand professional techniques used to identify customer needs and effective engagement and influence strategies

Module 17 – Cyber Security Awareness
Focus on the evolution of cyber threat, core threat groups, techniques and mitigations when working with sensitive or legally protected data

Module 18 – Logic and problem solving day
An "away day" with focus on implementation of key communication skills to control individual and team outputs in unfamiliar environments

Module 19 - Mental Health awareness
Overview of how to identify and support mental health and wellbeing of those within duty of care to improve personal and team effectiveness

Module 20 – Mock End Point Assessment
Preparation for End of Course End Point Assessment examination

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 Requirements:

Core Knowledge, Skills and Behaviours

Technical Competencies
Be able to undertake the following in line with organisational procedures and under supervision

- Identify, collect and migrate data to/from a range of internal and external systems
- Manipulate and link different data sets as required
- Interpret and apply the organisations data and information security standards, policies and procedures to data management activities
- Collect and compile data from different sources
- perform database queries across multiple tables to extract data for analysis
- Perform routine statistical analyses and ad-hoc queries

- Use a range of analytical techniques such as data mining, time series forecasting and modelling techniques to identify and predict trends and patterns in data
- Assist production of performance dashboards and reports
- Assist with data quality checking and cleansing
- Apply the tools and techniques for data analysis, data visualisation and presentation
- Assist with the production of a range of ad-hoc and standard data analysis reports
- Summarise and present the results of data analysis to a range of stakeholders making recommendations
- Works with the organisation's data architecture

Technical Knowledge and Understanding
- The range of data protection and legal issues
- The data life cycle
- The different types of data, including open and public data, administrative data, and research data
- The differences between structured and unstructured data
- The fundamentals of data structures, database system design, implementation and maintenance
- The importance of the domain context for data analytics
- The quality issues that can arise with data and how to avoid and/or resolve these
- The importance of clearly defining customer requirements for data analysis
- The processes and tools used for data integration
- The steps involved in carrying out routine data analysis tasks
- How to use and apply industry standard tools and methods for data analysis

Underpinning Skills, Attitudes and Behaviours
- Logical and creative thinking skills
- Analytical and problem solving skills
- Ability to work independently and to take responsibility
- Can use own initiative
- A thorough and organised approach
- Ability to work with a range of internal and external people
- Ability to communicate effectively in a variety of situations
- Maintain productive, professional and secure working environment

Data Technician Apprenticeship Standard

▶ **Level: 3**
▶ **Funding: up to £12,000**

Data technicians have a vital role within an organisation sourcing, formatting and presenting data for analysis using a different set of skills than those associated with the data analyst apprenticeship standard. The ability to communicate outcomes appropriate to the audience; analyse structured and unstructured data to support business outcomes; blend data from multiple sources as directed and apply legal and ethical principles when manipulating data is a skill set required within most large organisations. In their daily work, an employee in this occupation interacts with a wide range of stakeholders including colleagues, managers, customers and internal and external suppliers.

Our specialist tutors have designed an engaging delivery model that recognises these specialist skills and are confident that apprentices will gain significant new skills.

Modules Available:

Module 1 – Introduction to Data concepts and terminology
Understanding data types, formats, architecture and frameworks

Module 2 – Legislation and data management
Understanding core legislation, how to legally access, process, format and utilise data from a range of sources

Module 3-4 - Data Sources and Acquisition
Understanding the breadth of data sources available at various levels of the internet, how to safely and legally access, process and use this data within a corporate environment.

Module 5-12 – Applied Data phase
Familiarisation with a range of role and sector relevant data processing and analysis tools to collate, format and manage data for professional purposes. Programmes are specific to role but include Oracle, SQL, ARC, PowerBI, Bold BI, Tableau, SAP Analytics

Module 13 – Modelling data from multiple sources
Utilising skills developed in the Applied Data phase to collate and manage data from multiple sources across complimentary databases

Module 14 – Customer Insight and Effective Communication
Understand professional techniques used to identify customer needs and effective engagement and influence strategies

Module 15 – Cyber Security Awareness
Focus on the evolution of cyber threat, core threat groups, techniques and mitigations when working with sensitive or legally protected data

Module 16 - Mental Health awareness
Overview of how to identify and support mental health and wellbeing of those within duty of care to improve personal and team effectiveness

Module 17 – Mock End Point Assessment
Preparation for End of Course End Point Assessment examination

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

Knowledge, Skills and Behaviours

Knowledge

- Range of different types of existing data. Common sources of data - internal, external, open data sets, public and private. Data formats and their importance for analysis. Data architecture - the framework against which data is stored and structured including on premises and cloud.
- How to access and extract data from a range of already identified sources
- How to collate and format data in line with industry standards
- Data formats and their importance for analysis Management and presentation tools to visualise and review the characteristics of data Communication tools and technologies for collaborative working
- Communication methods, formats and techniques, including: written, verbal, non-verbal, presentation, email, conversation, audience and active listening Range of roles within an organisation, including: customer, manager, client, peer, technical and non-technical
- The value of data to the business How to undertake blending of data from multiple sources
- Algorithms, and how they work using a step-by-step solution to a problem, or rules to follow to solve the problem and the potential to use automation
- How to filter details, focusing on information relevant to the data project
- Basic statistical methods and simple data modelling to extract relevant data and normalise unstructured data
- The range of common data quality issues that can arise e.g. misclassification, duplicate entries, spelling errors, obsolete data, compliance issues and interpretation/ translation of meaning
- Different methods of validating data and the importance of taking corrective action
- Communicating the results through basic narrative
- Legal and regulatory requirements e.g. Data Protection, Data Security, Intellectual Property Rights (IPR), Data sharing, marketing consent, personal data definition. The ethical use of data
- The significance of customer issues, problems, business value, brand awareness, cultural awareness/ diversity, accessibility, internal/ external audience, level of technical knowledge and profile in a business context

- The role of data in the context of of the digital world including the use of eternal trusted open data sets, how data underpins every digital interaction and connectedness across the digital landscape including applications, devises, IoT, customer centricity
- Different learning techniques, learning techniques and the breadth and sources of knowledge

Skills

- Source and migrate data from already identified different sources
- Collect, format and save datasets
- Summarise and explain gathered data
- Blend data sets from multiple sources and present in format appropriate to the task
- Manipulate and link different data sets as required
- Use tools and techniques to identify trends and patterns in data
- Apply basic statistical methods and algorithms to identify trends and patterns in data
- Apply cross checking techniques for identifying faults and data results for data project requirements
- Audit data results
- Demonstrate the different ways of communicating meaning from data in line with audience requirements
- Produce clear and consistent technical documentation using standard organisational templates
- Store, manage and distribute in compliance with data security standards and legislation
- Explain data and results to different audiences in a way that aids understanding.
- Review own development needs
- Keep up to date with developments in technologies, trends and innovation using a range of sources
- Clean data i.e. remove duplicates, typos, duplicate entries, out of date data, parse data (e.g. format telephone numbers according to a national standard) and test and assess confidence in the data and its integrity.
- Operate as part of a multi-functional team
- Prioritise within the context of a project

Behaviours

- Manage own time to meet deadlines and manage stakeholder expectations
- Work independently and take responsibility
- Use own initiative
- A thorough and organised approach
- Work with a range of internal and external customers
- Value difference and be sensitive to the needs of others

Security First Line Manager

▶ **Level: 3**
▶ **Funding: up to £6,000**

Our extensive military, policing, retail and security sector experience has identified numerous opportunities in which specialist security and security management skills can be improved. Our engaging delivery model will allow apprentices to become competent in supervising people and activities in line with regulatory requirements; undertaking security risk assessments; providing security advice to others; understanding threat, vulnerability and risk; security methods, operations and activities; incident management and planning; stakeholder management; business communications and data security management within role(s) such as Ministry of Defence, Transport & Border Security and Private Security Industry. Understanding the threat, vulnerability & risk on a local, national and international security basis, and how to respond accordingly, would offer candidates a significant advantage over others with general managerial skills.

Modules Available:

Module 1 – Relevant Legislation, guidance, governing bodies
Provides full oversight and evaluation of legislation and best practices associated with safe and effective security supervision.

Module 2/3 – Risk Management within the Security Environment
Risk management principles and models, risk management techniques, health and safety risk, security risk

Module 4/5 – Scenario generation techniques
Practical application of analytical techniques used by intelligence services to identify, mitigate and respond to risk. Risk forecasting. SWOT, Cone of Plausibility, Backcasting, Analysis of Competing Hypothesis.

Module 6 – Effective Decision Making
A range of decision making models, decision making cycle, Effective recording and decision making audit trails

Module 7 – Managing in a security focused environment
Evaluation of core leadership and management styles and their relevance within your security environment. Identification of situational leadership and appropriate application.

Module 8 – Personnel management and professional development
Learning how to manage and develop your staff to increase team effectiveness and collaboration.

Module 9 – Effective Communication
Learning how to promote effective verbal and non-verbal communications within teams. Understanding behavioural traits, maximising influence and maintaining professional relationships.

Module 10 – Cyber Security and Communication security
Understanding the evolution of cyber threats, threat actors and mitigations. Focus on security equipment and infrastructure vulnerabilities and best practices.

Module 11 – Operational Team Leading Day
Off site Team Leading Day with focus on development of core skills within a non-familiar environment

Module 12 – Mental Health awareness
Overview of how to identify and support mental health and wellbeing of those within duty of care to improve personal and team effectiveness

Module 13 – Mock End Point Assessment
Preparation for End of Course End Point Assessment examination

Module 14 – Portfolio Review
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

Knowledge
Assessing and controlling risks in relation Health & Safety. Have complete understanding of current health and safety regulations, with a view to minimising H&S risks and hazards to health and wellbeing, relevant to the Security Context/ Environment in which you operate e.g private Security Industry, MOD, Event Security, 'in –house', Dept for Transport,. Recognise the security needs of Customers and Stakeholders, and effect appropriate solutions.

- Understand the market in which the role operates and the specific needs of each customer/industry stakeholder, thus developing strong customer relationships and confidence in the security provision.
- Identify and assess possible threats and take relevant action.
- Understand the Organisational structure, policies & procedures as well as potential threats to the industry, modus operandi of individuals and specific organisations, both internally and externally.
- Manage Staff performance, development and welfare.
- Awareness of the role requirements and individual knowledge & skills and security specific accreditation/certification of personnel needed to carry out their role within the Security Environment.
- Understanding of Employment law, human rights, policies and procedures governing people management, and knowledge of leadership & motivational theories and principles.
- Review security service provision against agreed KPIs, action within relevant regulations and guidelines
- Knowledge of relevant regulations governing security on a local and national scale. Understand areas of development that need to be addressed, of a security nature, in relation to specific customer needs.
- Manage outcome of service review and take action
- Understand concerns surrounding issues, threats and risk and be aware of available options.
- Ensure compliance with regulations and provide advice/solutions to potential security risks.
- Understand the regulations governing Security on a local, National and, where appropriate, international scale.
- Know how to identify and assess strengths, weaknesses, opportunities, risks, vulnerabilities and complex threats to security operations
- Ensure security of Communication
- Be conscious of the need for the appropriate use of written/verbal communication in all areas of security, including effective use of radios. Control access to customer & client information , security details, alarm codes, keys etc
- Manage Community Social Responsibility
- Know the impact and effects that your industry has on the environment and your responsibility to that community.
- Understand the importance of linking in with intelligence sources and crime/threat reduction initiatives.
- Control security of Office/Site/Venue
- Understand the customer's area of responsibility in order to provide the correct level of protection of all buildings and assets
- Manage Expectations
- Understand the 'bigger picture'. Be aware of how your role impacts on others and the Security Environment.
- Effective deployment of resources
- Awareness of all personnel and equipment in your area of responsibility e.g Screening equipment, radios, CCTV equipment, barriers etc

Skills

- Application of Health and Safety legislation in a security environment
- Application of health and safety policies & practices, ensuring compliance with all legislation and regulations whilst minimising risks and threats derived from operating in a security related role.
- Manage Customer/Clients/Stakeholders
- Ability to deliver a specific solution to meet the security needs of customer/industry stakeholder. Develop strong relationships and demonstrate competence & reliability in relation to security solutions and advice.
- Respond to Threats
- Identify and manage the threat effectively and use appropriate resources to reduce risks to the customer/organisation
- Ensure Staff are competent to operate within the security industry.
- The ability to interact with and manage people professionally and with integrity, whilst remaining compliant with all National and International Security regulations and guidelines, employment law and Human Rights Act. Providing coaching and guidance to instil confidence and competence within the workforce.
- Undertake Review
- The ability to review and effect change in relation to analysis of information/intelligence, feedback received, of a security nature.
- Manage Outcomes/Problem Solving
- Formulate and implement improvements to security, in order to reduce issues, address threats and minimise risk
- Ensure Compliance
- Compliance with all organisational security operations, policies, and procedures, utilising identified best practices and risk management principles. Take action to address non- compliance.
- Manage Communication
- The ability to communicate effectively on all levels, in various formats, both internally and externally, particularly during crisis management, incident reporting, liaising with other providers, such as Emergency Services.
- Encourage Community Social Responsibility
- Identify and implement effective measures to reduce/minimise risk and promote community social responsibility
- Manage Office/Site/Venue
- Ability to dispatch/provide a sufficient level of security in order to protect the customer's assets in all circumstances including lone working, under duress and in hostile environments.
- Manage Expectations
- Deliver solutions to meet specific security expectations, to ensure successful completion of responsibilities.
- Manage Resources/Planning and Organising.
- Utilise resources effectively, without injury or loss, in order to ensure full delivery of Security Service standards.

Risk/Compliance Officer Apprenticeship Standard

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

The Risk/Compliance Officer Standard was developed to provider 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.

knowledge, skills and behaviours associated as below:

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.

Phone: 01234 381660

Email: info@intelligenciatraining.com

Intelligencia Training Limited
3 Appley Court
Haynes
Middlesex
Bedfordshire
MK45 3QQ

www.intelligenciatraining.com