ST0967/V2

Draft assessment plan for the Data protection and information governance practitioner apprenticeship

Apprenticeship reference number	Level of this assessment (EPA)	Integration
ST0967	4	None

Assessment Plan

Assessment details

Introduction

This Apprenticeship Assessment Plan (AAP) sets out the requirements for the assessment of the Level 4 data protection and information governance practitioner apprenticeship. It should be read in conjunction with the General Requirements for Apprenticeship Assessment. Where there is conflict between this AAP and the General Requirements, this AAP takes precedence. Assessment organisations must also comply with the relevant regulatory framework for apprenticeship assessment.

It is important that the assessment of apprentices is proportionate, valid, and provides reliable evidence of an apprentice's attainment of the relevant knowledge and skills. As such, assessment organisations must design assessments to ensure:

- employers have confidence that the apprentice has reached the expected performance standard
- apprentices are sufficiently secure in their knowledge and skills, so that they could demonstrate their competence in different contexts (for example, a different workplace)

Assessment Outcomes

The assessment outcomes group and summarise the knowledge and skills that must be demonstrated in assessments. All assessment outcomes must be assessed.

Knowledge and skills statements in **bold** are mandatory and must be assessed in every version of the assessment that is made available.

Assessment Outcome	Mapping
AO1: Data Protection and Regulatory Compliance Interprets and applies data protection legislation and regulatory requirements (e.g., GDPR, FOI) in organisational contexts. Advises stakeholders, prepares documentation, and makes decisions on compliance issues.	**K1*, K7***, K8*, K12*, S3*, **S7***, S8, S9*, **S12**
AO2: Information Governance and Risk Management Conducts risk assessments and applies governance frameworks to manage information governance and data protection risks. Investigates data incidents and breaches and recommends appropriate mitigation strategies aligned to organisational risk appetite and priorities.	**K4***, K5, K9, S10, **S11***
AO3: Data Handling and Technology Operations Uses IT systems and software to collect, analyse, store, and present data securely. Applies privacy by design principles and identifies potential technical solutions to improve data management.	**K2***, K3, K6, **S1**, S6*, S14*
AO4: Stakeholder Engagement and Communication Communicates complex regulatory and technical requirements clearly through reports, presentations, and consultations. Provides training and guidance to stakeholders and influences compliance recommendations in line with organisational culture and priorities, supporting organisational compliance activities.	**K11***, K13*, K14*, **S2*,** S13*

AO5: Continuous Improvement and Horizon Scanning Manages competing priorities and adapts to changing organisational needs while maintaining compliance and delivering organisational value. Identifies opportunities for improving systems and processes by monitoring legislative, regulatory, and industry developments with an appropriate level of awareness of relevant legislative and case law developments for the role.	K10, K15, **K16***, S4, **S5**

(*) Knowledge and skills statements which offer opportunities to develop functional English and maths are identified with an asterisk.

<u>Assessment requirements</u>

Assessment organisations must set apprenticeship assessments. Assessment organisations should consider how technology and digital tools can support innovation and efficiency.

Assessment organisations must design apprenticeship assessments to include one **Project** and, if applicable, any relevant constraints. The Expert Group have expressed a preference that assessment organisations should consider using a presentation with questions and answers as additional methods alongside the project as they naturally align.

Any additional assessment(s) must be selected from the following list of methods to ensure the assessment outcomes are met in full:

- Interview
- Professional discussion
- Question and answer
- Presentation
- Project
- Written assessment (Short answer, long answer, essay, case study, reflective journal)
- Portfolio

Apprentices may be assessed at any appropriate point during their apprenticeship programme.

Assessments may be designed to allow a centre or training provider to mark assessments. The assessment organisation is responsible for ensuring all assessments are sufficiently reliable and valid, and for the accuracy of any centre or training provider marking.

<u>Performance descriptors</u>

Performance descriptors describe the level of performance required to achieve a pass or distinction grade. Assessment organisations must design assessments that align with these descriptions.

Takes responsibility for own actions and decisions within defined parameters, managing workload and meeting statutory deadlines (e.g. DSARs, incident/breach reporting) while escalating issues appropriately and operating within organisational risk and escalation frameworks.

Performance Category	**Pass**	**Distinction**
Applied knowledge	Demonstrates sound application of data protection and information governance knowledge (e.g., GDPR, FOI, privacy by design) to address compliance and operational issues, producing appropriate and reliable outcomes, including awareness of relevant legislative and case law developments appropriate to the role.	Applies regulatory and technical knowledge with confidence and precision, drawing on relevant legislative and case law developments where appropriate, to deliver solutions that meet compliance requirements and measurably improve organisational processes or stakeholder assurance.
Applied Skills	Selects and applies suitable investigative, analytical, and technical skills to manage data incidents and breaches, conduct DPIAs, and prepare compliance documentation, consistently and effectively using methods appropriate to the evidence available in their organisational context.	Selects and applies investigative, analytical, and technical skills to manage complex or high-risk data incidents, demonstrating flexibility and fluency in optimising approaches. Delivers measurable impact through efficiency gains, risk reduction, or improved compliance outcomes aligned to organisational priorities.
Regulatory and Procedural Awareness	Applies relevant legislation, regulatory frameworks, and organisational procedures (e.g., incident/breach reporting, retention schedules) with sound judgment, ensuring compliance in varied and occasionally complex scenarios, and calibrating responses to organisational risk appetite.	Interprets and applies regulatory and procedural requirements with insight, anticipating implications and proactively recommending improvements, calibrated to organisational risk appetite and escalation routes, to governance frameworks and compliance processes in complex or evolving situations.

Communication and Collaboration	Communicates clearly and accurately with internal and external stakeholders, explaining complex requirements in accessible terms and supporting compliance activities through effective collaboration.	Communicates and collaborates with confidence and adaptability, tailoring approach to diverse stakeholder needs and organisational culture, influencing compliance recommendations to maximise adoption and improve organisational compliance and stakeholder engagement.
Information Use and Decision Making	Analyses and interprets data and regulatory information to make informed decisions on compliance issues, risk mitigation, and the management of data incidents and breaches, demonstrating awareness of organisational priorities and risk appetite.	Evaluates and applies information from multiple sources (including organisational data about incidents) to justify decisions with insight, anticipating broader implications and recommending strategic, risk proportionate improvements where appropriate.
Responsibility and Autonomy	Takes responsibility for own actions and decisions within defined parameters, managing workload and meeting statutory deadlines (e.g., DSARs, incident breach reporting) while escalating issues appropriately and operating within organisational risk and escalation frameworks.	Proactively takes responsibility for decisions and actions within their role's remit, managing own work and coordinating others where required. Demonstrates sound judgment in balancing risks and priorities in line with organisational risk appetite to deliver compliance and organisational value.

Professional recognition

This apprenticeship aligns with the professional body recognition detailed in the occupational standard.

Please contact the relevant professional body for further information.