Level: Developing/Skilled

Information Security Grade 6

Typical roles: Information security Analyst, Tier 1 SOC Analyst

Experiences

Activities and responsibilities likely to be required when working at this level

Applies and maintains specific security controls as required by organisational policy and local risk assessments; Communicates security risks and issues to managers and others. Performs basic risk assessments for small information systems; Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures; Supports investigation of suspected attacks and security breaches.

Personal and professional development

This is the entry level for staff who are new to security.

Learning on the job

ISG work across UCL team members at this level are expected to broaden their knowledge of UCL, familiarise themselves with the team playbook for responding to common issues and learn where to escalate more complex matters.

Learning from others

As team members identify areas, they would like to consider specialising in they will work more closely with staff in those areas to develop the relevant skills whether those be in an aspect of security operations or GRC.

Formal learning

Security+ certification. Any of the certifications listed for Grade 7. Relevant material from LinkedIn Learning or the library of training material held by the team.

UCL Ways of Working

These describe expected behaviours in line with UCL culture and values (see pages 54-55).
For Ways of Working indicators and steps to development please refer to the Ways of Working website www.ucl.ac.uk/human-resources/policies-advice/ways-working

Transferable skills and competencies

PLANNING AND ORGANISING

FOLLOWING INSTRUCTIONS AND PROCEDURES

WORKING WITH PEOPLE

(See pages 52-53)

Level: Independent

Information Security Grade 7

Typical Roles: Information Security Officer, Tier 2 SOC Analyst

Transferable skills and competencies

ANALYSING

FOLLOWING INSTRUCTIONS AND PROCEDURES

PRESENTING AND COMMUNICATING INFORMATION

(See pages 52-53)

Experiences

Activities and responsibilities likely to be required when working at this level

Provides guidance on the application and operation of elementary physical, procedural, and technical security controls; Explains the purpose of security controls and performs security risk and impact analysis for medium complexity information systems; Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks; Investigates suspected attacks and supports security incident management.

Personal and professional development

Development options to consider when working towards this level

Learning on the job

Grade 7 staff will be expected to be the team expert on their area of specialisation. They will be move from following the team playbook to recommending changes to it. A key aspect of their role will be learning how to apply the general theory they have studied to the specific environment and issues of UCL.

Learning from others

Team members will continue to learn from more senior colleagues and to cross train in other areas of security which interest them. Building an understanding of the needs and drivers for the teams they most commonly interact with.

Formal learning

CISSP, CISM, ISO27001 auditor, GCIH, GCNA or other relevant SANS course. Relevant material from LinkedIn Learning or the library of training material held by the team.

UCL Ways of Working

These describe expected behaviours in line with UCL culture and values (see pages 54-55).
For Ways of Working indicators and steps to development please refer to the Ways of Working website www.ucl.ac.uk/human-resources/policies-advice/ways-working

Level: Advanced

Information Security Grade 8

Typical Roles: Senior Information Security Officer, Tier 3 SOC Analyst, Vulnerability Manager

Experiences

Activities and responsibilities likely to be required when working at this level

Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards; Contributes to development of information security policy, standards and guidelines; Obtains and acts on vulnerability information and conducts security risk assessments, impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements; Develops new architectures that mitigate the risks posed by new technologies and organisational practices.

Personal and professional development

Mentoring, presenting, ability to organise and delegate work.

Learning on the job

Staff at this level will hold significant responsibility, for example delivery of all vulnerability management and pen testing services. To do this effectively they will need to broaden their understanding from the area of specialism their delivered at Grade 7 to understand a wider field of study.

Learning from others

Understanding of the specialist areas under their remit.

Formal learning

Additional courses from the material discussed at Grade 7.

UCL Ways of Working

These describe expected behaviours in line with UCL culture and values (see pages 54-55).
For Ways of Working indicators and steps to development please refer to the Ways of Working website www.ucl.ac.uk/human-resources/policies-advice/ways-working

Transferable skills and competencies

RELATING AND NETWORKING

FORMULATING STRATEGIES AND CONCEPTS

PERSUADING AND INFLUENCING

(See pages 52-53)

Level: Senior

Information Security Grade 9

Typical Roles: SOC Manager, Head of Risk and Governance, Security Domain Architect

Transferable skills and competencies

LEADING AND SUPERVISING

RELATING AND NETWORKING

FORMULATING STRATEGIES AND CONCEPTS

(See pages 52-53)

Experiences

Activities and responsibilities likely to be required when working at this level

Develops and communicates corporate information security policy, standards, and guidelines; Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards, and guidelines; Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on strategies, benefits, and risks; Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.

Personal and professional development

Management and Leadership skills.

Learning on the job

Networking and communication skills due to the extensive outreach at this level.

Learning from others

Due to the amount of outreach carried out at this level learning from other teams which engage outside ISD is essential.

Formal learning

security course, UCL leadership programmes, TOGAF and/or SABSA for architects.

UCL Ways of Working

These describe expected behaviours in line with UCL culture and values (see pages 54-55). For Ways of Working indicators and steps to development please refer to the Ways of Working website www.ucl.ac.uk/human-resources/policies-advice/ways-working