

Annex A.

Business Safety Resilience

Graduate International Certified Security Practitioner Capabilities

Security Risk Analysis

- Proficient in using methodology to determine and prioritise, security risk through the analysis of threat, vulnerabilities and impact.
- Capable of selecting, for each identified risk, appropriate and economical risk management approaches that will reduce risk to as low as reasonably practicable.
- Demonstrate through metrics that the chosen risk management strategy will deliver a return on investment.

Facility Counterterrorism

- Understanding the range of terrorist tactics that are employed to attack an organisation.
- Having the ability to optimise standard security measures to mitigate the most common kinds of terrorist action.
- Able to identify and specify those specific counterterrorism protective security measures necessary to address specific terrorist actions that can be mitigated by the optimisation of existing security means.
- Able to deliver training and development to staff and business on recommended actions by staff and personnel in the event of a terrorist or similar violent attack.

Crime & Loss Prevention

- Advanced understanding of the drivers of crime, and the associated key crime motivation theories.
- Able to select different crime prevention and management approaches to address both externally and internally perpetrated crimes. The approaches will be grounded in the best-known and most successful crime prevention theories, based on latest research.
- Able to apply the best principles of environmental design to create a crime tranquil environment.

Managing the Security Function

- Execution of the core skills necessary to manage a security function and able to advise customers on how to carry this function out effectively to achieve target solutions.
- Able to focus the security programme correctly, using the most appropriate mix of hardware, procedures and personnel.
- Able to match the security programme with the culture of the organisation, cross-network with managers to establish a collaborative approach to security risk management, with the ability to present the benefits of the programme to senior management.

Leadership and Management (GCGI)

- Understands the key differentiating factors between management and leadership and has the ability to put leadership good practice into effect.
- Studied extensively the core theories on motivation and has the ability to apply these to ensure maximum productivity from the security team.
- Understands the dynamics of teamwork and the key underpinning theories and is able to organise personnel into effective teams and leverage the dynamics that teamwork can deliver to the benefit of the organisation.

Security Design, Evaluation and Surveying

- Application of the fundamental set of principles that underpin every security design and is able to apply these to produce an optimally configured security programme that is in harmony with the culture of the organisation and its mission objectives.
- Able to evaluate the effectiveness of security systems and programmes against a defined set of parameters.
- Able to survey the organisation's security systems to identify areas of imbalance between risk and security and to make appropriate recommendations to optimise security resources; in order to achieve greatest risk mitigation at an economical cost.

Perimeter Protection

- Able to select from a range of perimeter protection options to design a perimeter which is appropriate to the culture and mission of the organisation and which reduces risk of intrusion to as low as reasonably practicable.
- Understands the range of surveillance, detection and delay technology available and is capable of; selecting the right technologies for given circumstances and integrating all perimeter design elements to create an optimal protective design.
- Understands the inherent vulnerabilities of perimeters and is capable of; advising how to integrate and configure manpower to create an effective perimeter defense that provides appropriate deterrence and credible response to incursion attempts.

Protecting Buildings

- With a total understanding of the range of crimes, security risks and vulnerabilities associated with buildings, is able to, recommend security measures that are in harmony with the occupants need for health and safety.
- Able to select appropriate security measures for a range of building types and functions, from single-occupier, multi-tenant, old and new with a range of operations from high-risk industrial to retail.

- Able to apply or advise on appropriate security measures to meet the specific requirements of varied internal building environments. Measures include environmental design to reduce opportunities for crime, security hardening measures, locking systems, intrusion detection and assessment, incident response and surveillance.

Access Management

- Able select from a range of different access management approaches and regimes for a wide range of environments and functions.
- With a full understanding of the primary equipment, technology and methods necessary to create effective access management can specify and apply these proficiently.
- Able select from a range of mechanical, electronic, biometric locking and access management devices and understands how and where each can best be utilised, while ensuring conformance with building regulations and fire codes for both conventional and complex buildings.

Surveillance (CCTV)

- Able to differentiate between the pros and cons of the multitude of different CCTV surveillance options available.
- Able to produce a specification for a CCTV surveillance concept for a range of circumstances, whilst taking-into-account; developments in technology and associated economical payback through diversified and dynamic return on investment.
- Through the correct and cost-effective application of CCTV surveillance the able to reduce the exposure of the organisation to crime and loss.

Protection of Information

- Able to advise line and senior management on a range of current and emerging threats to information in hardcopy and electronic form, and advise on the unique respective implications of targeting trade secrets, proprietary information and personal data.
- Able to recommend a range of human, technical and procedural countermeasures designed to reduce the exposure of sensitive information to compromise.
- Understands and can advise on threats to information in specific circumstances (e.g. travel, telephonic, spoken in meeting rooms and office etc.) and can advise on specific counter-technical surveillance measures to address each.

Protection of at-Risk Personnel

- Production of policies and programmes designed to manage workplace violence risk.
- Able to specify a range of security measures to reduce exposure to the spectrum of robbery in cash-handling and other vulnerable areas.
- Able to develop proactive programmes and emergency response measures which will be implemented in the event of an active shooter or disturbed person(s) with weapons on site.
- Able to implement a programme of measures designed to manage the security of business travelers while overseas.
- A specialist adviser in close protection of personnel in all environmental conditions.