GIAC GSLC PREPARATION COURSE - Module Structure

- **Module Title:** Course Introduction
- **Description:**

This advanced-level certification validates the certification holder's understanding of information security management, technical controls and governance with a specific focus on detecting, responding and protection against information security issues. GSLC verifies expertise in data, network, application, host, user controls, as well as security life cycle management topics. The certification is intended for information security managers, information security professionals with leadership, or managerial responsibilities and information technology management.

- **Learning outcomes:**

Participants will gain an understanding of the general outline of the GIAC certification process, including the exam format. They will be aware of the resources available to assist them in building their knowledge to a level that will enable them to enroll for the GIAC GSLC examination.

- **Lecture title:**

GIAC GSLC Security Leadership Certification Course Introduction

- **Lecture description:**

This session introduces the overall GIAC GSLC course and provides the course curriculum roadmap. Information relating to the profile of attendee that GIAC foresees being suited to this course is provides. The areas covered within the GSLC course that are required for certification are included. An outline of how to take the examination and the outline of the course content is illustrated.

GIAC GSLC PREPARATION COURSE - Module Structure

- **Module 1 Title:** 01. Mal Actors & Attacks

- **Description:**

Cyber attacks are undertaken by mal actors with different profiles and it is important to understand which profile of adversary is targeting an organization. Without comprehending this aspect of cyber security, incorrect risk assessments and assignment of inappropriate cyber security controls may result. By identifying various types of attack vectors and likely impacts within an entity, cyber security resources can be more efficiently attributed. This session provides insight into why and what mal actors are seeking to achieve, as well as their motivation for executing particular types of attack.

- **Learning outcomes:**

Participants will gain an understanding of the rationale for specific forms of cyber-attack, as well as gaining knowledge of where within all entities a cyber-attack may impact. An overall comprehension of the overall context within which the cyber and IT security domains function is attained.

- **Lecture title:**

Mal Actors & Attacks

- **Lecture description:**

This introductory session demonstrates the operating environment facing all entities today, in respect of attackers, their motives and impacts resulting from cyber breaches. Participants are provided with the details of who is behind cyber attacker's actions, as well as the wide-reaching financial, compliance, 3rd party and reputational damage facing organizations where their cyber and IT security experiences a lapse.

- **Module 2 Title:** 02. Risk Management & Security Frameworks & Standards
- **Description:**

There are a number of standards and frameworks available to reduce, or eliminate cyber and IT security risks, ranging from being highly detailed and technical, to general, or generic standards. Which to utilize and for which purpose is described sufficiently, to encompass coverage overall of the generally accepted standards and frameworks on an international basis.

- **Learning outcomes:**

Participants will have knowledge of the various standards and frameworks that contribute to enhancing cyber security within any entity, from both a technical and organizational perspective. They will comprehend which frameworks and standards can be most beneficial according to the specific areas being targeted for security uplift. For the GSLC, it is necessary to have an awareness of what standards and frameworks are available to utilize within the role of a security professional and how they may be applied.

- **Lecture title:**

  Risk Management & Security Frameworks & Standards
- **Lecture description:**

The standards and frameworks that are globally accepted as the benchmarks for implementation within any organization that can improve cyber resilience are covered. These include ISO, NIST, OCTAVE, COBIT, ENISA, CIS controls and others within the risk assessment domain. In many instances, certain standards are mandated by law, for

example within government agencies. Others can be applied on a piecemeal, or ad hoc basis, whilst developing cyber security maturity.

Through the session, there is an evaluation of how to ensure management of cyber risks is in alignment with business objectives through the adoption of security frameworks and risk management techniques, in order to assist in maturing an organization's cyber security program.

Implementation of the available standards and frameworks is not covered, since this does not fall within the scope of the GSLC examination curriculum.

- **Module 3 Title:** 03. Managing Awareness Part 1
- **Description:**

The greatest cause of successful cyber breaches arises from human error. This may manifest through a lack of skills and experience, as well as through personnel disregarding an organizations' policies and procedures. It is for this reason that international standards, such as ISO27001 and 27002, along with best practice frameworks such as the NIST 800 series for cyber security guidance have been revised in recent times to reflect this critical aspect of building robust cyber security programs within all entities. This session covers how such awareness may be developed.

- **Learning outcomes:**

The participant will be able to assess an organization's human risks and build a security awareness program that can mature with the organization's security program. Those with managerial or supervisory responsibilities will be competent to plan and manage security

projects and initiatives across multiple personnel profiles, in order to change behavior and build a security-aware culture.

- **Lecture title:**

  Managing Awareness Part 1

- **Lecture description:**

This session provides the knowledge for a professional to be able to establish a minimum standard of security knowledge, skills, and abilities across an organization. The session content delivers the information required to gain comprehension of the underlying critical elements of creating and managing a cyber security awareness program. It includes the background to cyber-attacks, how cloud computing creates new forms of risks and how the cyber attack cycle has shifted in more recent periods to create awareness of the cyber kill chain.

- **Module 3 Title:** 03. Managing Awareness Part 2

- **Description:**

The greatest cause of successful cyber breaches arises from human error. This may manifest through a lack of skills and experience, as well as through personnel disregarding an organizations' policies and procedures. It is for this reason that international standards, such as ISO27001 and 27002, along with best practice frameworks such as the NIST 800 series for cyber security guidance have been revised in recent times to reflect this critical aspect of building robust cyber security programs within all entities. This session covers how such awareness may be developed.

- **Learning outcomes:**

The participant will be able to assess an organization's human risks and build a security awareness program that can mature with the organization's security program. Those with managerial or supervisory responsibilities will be competent to plan and manage security projects and initiatives across multiple personnel profiles, in order to change behavior and build a security-aware culture.

- **Lecture title:**

  Managing Awareness Part 2

- **Lecture description:**

This session covers various aspects of cyber-attacks, ranging from physical cabling, electromagnetic dangers, covert storage channels and rootkits. The module focuses upon malware and how it functions as a means of causing cyber security breaches, and/or impacting upon the CIA triad. Explanations of client-side versus server-side attacks is provided to enable a fuller understanding of the architectures utilized within the IT environment. Database security, IoT security and weaknesses within SCADA systems is disclosed.

- **Module 3 Title:** 03. Managing Awareness Part 3

- **Description:**

The greatest cause of successful cyber breaches arises from human error. This may manifest through a lack of skills and experience, as well as through personnel disregarding an organizations' policies and procedures. It is for this reason that international standards,

such as ISO27001 and 27002, along with best practice frameworks such as the NIST 800 series for cyber security guidance have been revised in recent times to reflect this critical aspect of building robust cyber security programs within all entities. This session covers how such awareness may be developed.

- **Learning outcomes:**

The participant will be able to assess an organization's human risks and build a security awareness program that can mature with the organization's security program. Those with managerial or supervisory responsibilities will be competent to plan and manage security projects and initiatives across multiple personnel profiles, in order to change behavior and build a security-aware culture.

- **Lecture title:**

  Managing Awareness Part 3

- **Lecture description:**

This session covers overall management of organizational security awareness due to an increasing number of reasons as to why creating and cybersecurity awareness within all types of organizations is increasingly important. These range from international laws, such as the EU's General Data Protection Act, to state laws, such as the California Privacy Act of 2023, through to sectoral laws, such as the US CSRS, or the NIS and PSD2 in the EU, as well as sectoral regulations and standards, such as PCI DSS, as well as any number of data protection laws on a global basis, which have onerous financial penalties for data breaches. The module also covers hierarchical structures and reporting, plus the roles within IT departments.

- **Module 3 Title:** 03. Managing Awareness Part 4
- **Description:**

The greatest cause of successful cyber breaches arises from human error. This may manifest through a lack of skills and experience, as well as through personnel disregarding an organizations' policies and procedures. It is for this reason that international standards, such as ISO27001 and 27002, along with best practice frameworks such as the NIST 800 series for cyber security guidance have been revised in recent times to reflect this critical aspect of building robust cyber security programs within all entities. This session covers how such awareness may be developed.

- **Learning outcomes:**

The participant will be able to assess an organization's human risks and build a security awareness program that can mature with the organization's security program. Those with managerial or supervisory responsibilities will be competent to plan and manage security projects and initiatives across multiple personnel profiles, in order to change behavior and build a security-aware culture.

- **Lecture title:**

  Managing Awareness Part 4

- **Lecture description:**

This session explains the differences in the granularity, and nature, of information that is relevant to the different hierarchical levels within organizations. Without this understanding, there are risks not simply from sub-optimal utilization of information, but can lead to a misalignment of strategic intent with cyber security enhancements. The structures required

for effective cyber risk management within an organization's overall structure is discussed, allied with recent changes to structures resulting from generative AI, large language models and big data. Current and future cyber threat and technology advancements impacting upon cyber security within all entities is also covered in this module.

- **Module 4 Title:** 04. Managing Vendors
- **Description:**

With the increasing complexity of software vendors with the advent and rapid adoption of generative AI and large language models, coupled to other emerging and emergent technologies, vendor selection has a greater number of factors to be considered within the selection process. To implement new initiatives, security leaders must develop an awareness of all facets contained within vendor selection due diligence. Understanding the components that are required in conducting a thorough analysis of vendors is crucial for all organizations.

- **Learning outcomes:**

Participants will develop a broad view of all the elements that are required for analysis and assessment of software and system vendors, including technical, strategic and intellectual property considerations within an operating environment with high velocity for change. Understanding the risks associated with various development options, as well as compliance risks will be acquired.

- **Lecture title:**

  Managing Vendors

- **Lecture description:**

This session provides insight into how to manage vendors of either off the shelf commercial software and systems, or those that offer the services of developing proprietary code for an organization. This is not covered from a price negotiation basis, but rather in terms of managing the risks arising from vendors supplying products, code or services to entities.

Areas covered provide sufficient include insight into the areas that need to be accounted for during the purchasing due diligence process, ranging from intellectual property, to the security intrinsic within the products that are acquired by organizations. Software costs, risks, regulatory compliance, background checks as part of overall due diligence are covered within this session.

- **Module 5 Title:** 05. Managing Projects Part 1

- **Description:**

As a leader who is responsible for initiating, implementing and operating cyber security within an organization, understanding the different methods for organizing and running various types of cyber-related projects is key. By learning the core project management approaches of waterfall and agile methodologies and why each plays a separate role within the cyber domain, the correct selection aligns projects with organizational objectives. The effective control, reporting and structuring of various initiatives within an entity requires a basic command of project management.

- **Learning outcomes:**

The participant will have a fuller understanding of the fundamentals of project management methodologies, terminologies, the structure, responsibility and reporting requirements of projects in general terms. Comprehension of how to gain and retain support from the

business is gained. Application of different project management approaches is a core component of this session.

- **Lecture title:**

  Managing Projects Part 1

- **Lecture description:**

This session explains the differences between the two principal approaches to managing projects; the traditional waterfall method and agile, as well as why there are differing project management methods. The fundamental differences between approaches are discussed as well as disclosing the variance in the end goals of each one. The background and evolution of project management and the changes required for more dynamic deliverables requirements, along with specifications are also discussed in general terms in order to lead into the specific methods embodied within each method that are included within the overall Managing Projects course module.

- **Module 5 Title:** 05. Managing Projects Part 2

- **Description:**

This session explains the differences between the two principal approaches to managing projects; the traditional waterfall method and agile, as well as why there are differing project management methods. The fundamental differences between approaches are discussed as well as disclosing the variance in the end goals of each one. The background and evolution of project management and the changes required for more dynamic deliverables requirements, along with specifications are also discussed in general terms in order to lead into the specific methods embodied within each method that are included within the overall Managing Projects course module.

- **Learning outcomes:**

The participant will have a fuller understanding of the fundamentals of project management methodologies, terminologies, the structure, responsibility and reporting requirements of projects in general terms. Comprehension of how to gain and retain support from the business is gained. Application of different project management approaches is a core component of this session.

- **Lecture title:**

  Managing Projects Part 2

- **Lecture description:**

This session introduces the waterfall method of project management using the global standard approach of Prince 2. It describes the process and reporting structures within Prince 2, including the role of differing personnel, the business case, change management, the Prince 2 themes, tailoring and risks. The format follows standard Prince 2 basic training and enables any participant to structure complex projects with defined outcomes using the Prince 2 approach.

- **Module 5 Title:** 05. Managing Projects Part 3

- **Description:**

This session explains the differences between the two principal approaches to managing projects; the traditional waterfall method and agile, as well as why there are differing project management methods. The fundamental differences between approaches are discussed as well as disclosing the variance in the end goals of each one. The background and evolution of project management and the changes required for more dynamic deliverables

requirements, along with specifications are also discussed in general terms in order to lead into the specific methods embodied within each method that are included within the overall Managing Projects course module.

- **Learning outcomes:**

The participant will have a fuller understanding of the fundamentals of project management methodologies, terminologies, the structure, responsibility and reporting requirements of projects in general terms. Comprehension of how to gain and retain support from the business is gained. Application of different project management approaches is a core component of this session.

- **Lecture title:**

  Managing Projects Part 3

- **Lecture description:**

This session introduces the participant to the Dynamic Systems Development Method of Agile project management, with Agile being the primary approach for software and systems development on a global basis. The underlying principles of DSDM Agile are disclosed, together with the phases, roles and philosophy. The participant will comprehend how the Agile approach to project management differs fundamentally to the waterfall method, whilst also understanding how each fit to each other. The overall DSDM Agile methodology is presented in detail.

- **Module 5 Title:** 05. Managing Projects Part 4
- **Description:**

This session explains the differences between the two principal approaches to managing projects; the traditional waterfall method and agile, as well as why there are differing project management methods. The fundamental differences between approaches are discussed as well as disclosing the variance in the end goals of each one. The background and evolution of project management and the changes required for more dynamic deliverables requirements, along with specifications are also discussed in general terms in order to lead into the specific methods embodied within each method that are included within the overall Managing Projects course module.

- **Learning outcomes:**

The participant will have a fuller understanding of the fundamentals of project management methodologies, terminologies, the structure, responsibility and reporting requirements of projects in general terms. Comprehension of how to gain and retain support from the business is gained. Application of different project management approaches is a core component of this session.

- **Lecture title:**

  Managing Projects Part 4

- **Lecture description:**

The final session in this module summarizes the software packages available to project managers to facilitate their roles, whether fee-based, open-source local installations, or cloud-deployed options. An overview of the main players within the vendor sector. These include Atlassian, Asana, Project, Libre Project and a brief overview of the other options.

- **Module 6 Title:** 06. Managing A Cyber Program Part 1

- **Description:**

This session focusses upon IT and cyber security in relation to an organizations' ability to control such risks through its cyber and technology risk controls. These are critical to the maintenance of security and their analysis forms a substantial and increasing portion of external auditor analysis. Where such audits reveal potential weaknesses, leading to the possible questioning as to the accuracy of financial statement line items, then the mandatory accounts all organizations must file at least annually, will be impacted. As such, for both security and compliance reasons, ITGC's are crucial to any entity

- **Learning outcomes:**

The participant will be capable of designing a cyber security program, with an understanding of organizational structure, as well as best practice in terms of the reporting and program governance. They will acquire the knowledge required in managing personnel across various profiles and have a comprehension of the risk domains within an entity's cyber and technology areas.

- **Lecture title:**

  Managing A Cyber Program Part 1

- **Lecture description:**

This session introduces the area of technology security and technology risk management as requiring a unified approach and crossing several functional boundaries. The requisite integrated approach includes contextualization of the issues, as well as behavioral impacts. Different types of risk are discussed and the session includes defining roles and responsibilities within IT operations, allied to governance.

- **Module 6 Title:** 06. Managing A Cyber Program Part 2

- **Description:**

This session focusses upon IT and cyber security in relation to an organizations' ability to control such risks through its cyber and technology risk controls. These are critical to the maintenance of security and their analysis forms a substantial and increasing portion of external auditor analysis. Where such audits reveal potential weaknesses, leading to the possible questioning as to the accuracy of financial statement line items, then the mandatory accounts all organizations must file at least annually, will be impacted. As such, for both security and compliance reasons, ITGC's are crucial to any entity

- **Learning outcomes:**

The participant will be capable of undertaking a technology and cyber risk assessment exercise within an organization. They will have an awareness of the difference between a top-down and bottom-up risk assessment methods and where each is directed within an entity. They will have an understanding of mapping technology and cyber risks to attack surfaces, allied with comprehending threat vectors and defining cyber and technology control strengths.

- **Lecture title:**

  Managing A Cyber Program Part 2

- **Lecture description:**

This session introduces the participant to the methods of cyber and technology risk assessments, with a focus upon the top-down approach. Working through examples of actual threat data and how it is used in the assessment of threat exposures and capability of

risk controls within an organization is provided. Inherent, residual and control strength scoring is demonstrated and the rationale for measuring cyber security maturity is disclosed.

- **Module 6 Title:** 06. Managing A Cyber Program Part 3

- **Description:**

This session focusses upon IT and cyber security in relation to an organizations' ability to control such risks through its cyber and technology risk controls. These are critical to the maintenance of security and their analysis forms a substantial and increasing portion of external auditor analysis. Where such audits reveal potential weaknesses, leading to the possible questioning as to the accuracy of financial statement line items, then the mandatory accounts all organizations must file at least annually, will be impacted. As such, for both security and compliance reasons, ITGC's are crucial to any entity

- **Learning outcomes:**

The participant will have a full comprehension of how IT general controls, ITGC's operate to prevent security and operational issues within an entity. Knowledge of controls domains, control types, control categories, controls testing, control objectives, control design will be attained. Understanding of the prioritization and the associated risk register, for identifying key areas will be gained.

- **Lecture title:**

  Managing A Cyber Program Part 3

- **Lecture description:**

This session focusses upon IT general control domains and the rationale and functioning of them. A full discussion of the various facets of ITGC's is disclosed throughout this session, including how to evaluate the effectiveness and operational capability of an ITGC. How

GIAC GSLC PREPARATION COURSE - Module Structure

ITGC's are intended to manage cyber and IT risks through their testing and what is required to accompany ITGC evaluations is demonstrated. Security across IT functions, such as access to applications and data along with techniques for sampling and interviewing are also included within the session.

- **Module 6 Title:** 06. Managing A Cyber Program Part 4

- **Description:**

This session focusses upon IT and cyber security in relation to an organizations' ability to control such risks through its cyber and technology risk controls. These are critical to the maintenance of security and include software development controls, along with the three lines of defense models and segregation of duties, which are all fundamental to managing development and change risks. Program change and assessing risk management effectiveness create the ability to identify security weaknesses and to secure applications and data on an ongoing basis.

- **Learning outcomes:**

The participant will have an understanding of the software development lifecycle, SDLC. Comprehension of program change controls for managing change risks will be attained. Knowledge of segregation of duties, managing application security and the three lines of defense model will be attained, allied with reporting and understanding the stages of program change.

- **Lecture title:**

  Managing A Cyber Program Part 4

- **Lecture description:**

GIAC GSLC PREPARATION COURSE - Module Structure

This session covers areas of the software development lifecycle, from initiation to implementation. Controls for change management, together with an explanation of the three lines of defense model and segregation of duties are discussed. Risks and the management of change risks is disclosed, including walking through the program change stages, together with how to assess control effectiveness.

- **Module 6 Title:** 06. Managing A Cyber Program Part 5

- **Description:**

This session focusses upon how to develop appropriate data governance frameworks that take account of AI use within organizations that may lead to non-compliance regulatory breaches resulting from the use of big data, including personally identifiable data. Data management and big data governance is a major issue for entities seeking to leverage the benefits of artificial intelligence, but its use requires a rethinking of organizational structures and reporting lines to minimize compliance risks.

- **Learning outcomes:**

The participant will have an understanding of data governance within the developing products and services utilizing artificial intelligence, in conjunction with big data. Knowledge of how to build a data governance framework, along with the organizational structure required for effective data management is attained.

- **Lecture title:**

  Managing A Cyber Program Part 5

- **Lecture description:**

This session looks at the data governance frameworks required in an era of artificial intelligence and its' use of large language models requiring mass data, whilst still maintaining data privacy law compliance. The session highlights the requirements of using data for the provision of AI-powered products and services, in order to align with organizational objectives, whilst creating compliance risks. Examples of what is required for big data and blockchain technology usage is contained within the session.

- **Module 6 Title:** 06. Managing A Cyber Program Part 6

- **Description:**

This session focusses upon human errors, given that they are the primary cause of cyber and IT security breaches. Models of error, as well as reduction techniques are covered, along with how to build situational awareness within an organization. Factors impacting upon the probability of error occurrence are discussed.

- **Learning outcomes:**

The participant will have an understanding of the factors influencing the probability of human error within an organization. They will understand error distinctions, how to use different error -making models to assist in error reduction. Building cyber situational awareness skills will also be attained.

- **Lecture title:**

  Managing A Cyber Program Part 6

- **Lecture description:**

This session has a theme of human error running through it. Factors influencing human error probability, allied with preconditions required for error creation are disclosed. Methods and frameworks that seek to measure and predict human errors is included, together with

examples. The different forms of human error and causes of organizational errors and organizational drift are revealed, leading through to situational awareness within the cyber domain.

- **Module 7 Title:** 07. Security Architecture Part 1
- **Description:**

This section is on the security, architecture, and engineering aspects of technology and covers crucial areas such as access control, with its multiple formats that may confuse those without relevant explanation of them and their fit to an organization. The fundamental concepts of security models are covered, including setting of user access for access to data and applications.

- **Learning outcomes:**

The participant will comprehend the fundamental security models and modes of user access control and the way that these function within an entity in order to maintain elements within the CIA triad.

- **Lecture title:**

  Security Architecture Part 1

- **Lecture description:**

This session introduces the security fundamentals that apply within all organizations. There is a detailed description of the various forms of user access control, together with the strengths and weaknesses of them. Rules-based, role-based, lattice-based, discretionary, and mandatory access control forms are all disclosed. The generally accepted security models such as the Zachman framework, Bell la Padula, Graham-Denning and the Clark-Wilson models are all discussed.

- **Module 7 Title:** 07. Security Architecture Part 2
- **Description:**

This section covers secure design principles, in the same way that secure models were discussed in the previous session. The four primary principles underpinning overall technology and operational security are covered, along with additional principles. Various threat modelling techniques are revealed, followed by trust concepts. The secure architecture concept is also detailed within this session.

- **Learning outcomes:**

The participant will comprehend the fundamental secure design principles and their modes of implementation. An understanding of the secure architecture model, including overall computer hardware, as well as CPU and memory operation will be attained, along with knowledge of microservices and containerization.

- **Lecture title:**

  Security Architecture Part 2

- **Lecture description:**

This session introduces the participant to security design principles and secure architecture models that underpin computer security. Areas covered in the session include the impact of data privacy laws that determine the CIA triad and how security is applied within organizations. Zero trust principles, privacy by design and overall secure architecture concepts and security domains are included. Hardware architecture and its operation are discussed, along with how CPUs operate and what risks are posed to different forms of

architecture. Threat modelling methods, such as TRIKE, PASTA, STRIDE and DREAD are explained, together with risks arising from virtualization and cloud shared responsibilities.

- **Module 8 Title:** 08. Cryptography Concepts for Managers Part 1
- **Description:**

This session covers building an understanding of cryptography concepts, encryption algorithms, and the application of cryptography, which is a foundational element of creating a secure system. With the rise of data privacy as a major issue, resulting in more personal data laws on a global basis, how encryption may be utilized in conjunction with meeting the requisites of the CIA triad are discussed.

- **Learning outcomes:**

The participant will acquire the knowledge of common cryptographic terminology, to build an understanding of how symmetric, asymmetric, and hashing encryption works. They will understand how encryption to secure data in transit or at rest is utilized, and also how to identify and address privacy and compliance requirements.

- **Lecture title:**

  Cryptography Concepts for Managers Part 1

- **Lecture description:**

This session introduces the principles and operation of cryptography algorithms and their concepts. Several cryptographic algorithms and the concepts underpinning secure ciphers are disclosed and explained. The application of cryptography, including within VPN's and IPSec are included. The basic definitions of cryptography and hashing are explained in a

manner that is comprehensible within a domain of complexity. Hash functions, salting and nonce's are also covered.

- **Module 8 Title:** 08. Cryptography Concepts for Managers Part 2
- **Description:**

This session covers building an understanding of cryptography concepts, encryption algorithms, and the application of cryptography, which is a foundational element of creating a secure system. With the rise of data privacy as a major issue, resulting in more personal data laws on a global basis, how encryption may be utilized in conjunction with meeting the requisites of the CIA triad are discussed.

- **Learning outcomes:**

The participant will build a basic understanding of the fundamental terminology and concepts of cryptography. The various forms of cryptographic attack will be understood, as well as how cryptography is implemented within organizations. Knowledge of public key infrastructure, IPV4 and IPV6 and CA's will be attained.

- **Lecture title:**

Cryptography Concepts for Managers Part 2

- **Lecture description:**

This session illustrates how public and private key infrastructure works, allied with certification authorities. The most common forms of cryptographic attacks are explained. These include reference to key stretching, brute force, digraph and frequency analysis attack methods. Differences in protocols, such as between IPV4 and IPV6 are disclosed and cryptanalysis is covered in sufficient detail to form a sound understanding of the

fundamental issues, implementations and management of cryptographic systems within an organization.

- **Module 9 Title:** 09. Business Continuity Physical Security Part 1
- **Description:**

In this session, the discussion of longer-term business continuity planning and disaster recovery requires an understanding by managers that physical security requires risk controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. Many of the technology-oriented security risk mitigation controls can fall vulnerable to ostensibly non-technology designed attacks and security failures.

- **Learning outcomes:**

The participant will gain a fuller understanding of how managing business continuity relates to physical security components within a BCM environment. Comprehension of how technological security controls may be bypassed, or negatively impacted by multiple facets of physical security compromise will be attained.

- **Lecture title:**

  Business Continuity Physical Security Part 1

- **Lecture description:**

This session concentrates upon how physical security extends across a number of different areas, whilst forming part of the security design-in-depth model when business continuity plans are being developed. Physical aspects of risk posed to an organization are addressed through having a number of controls applied to them. Coverage here includes for

preventative controls, including perimeter defenses, how door locks may be compromised, as well as detective controls that may be comprised of CCTV systems, alarm systems, that may have motion sensors, heat sensors, and smoke sensors. Additionally, subjects such as fences, security guards, dog's lights, signage are explained and how each may fit within both deterrent controls and preventative ones. The final area of coverage is on compensating controls. Risks that are inherent are also disclosed, allied to business continuity in respect of geographical impacts and considerations when establishing backup data centers.

- **Module 9 Title:** 09. Business Continuity Physical Security Part 2
- **Description:**

When business continuity, recovery and reinstatement of systems and data are discussed, there is a general line of thought of the more technological aspects to maintaining resilience through redundancy, offsite backups, and so forth. However, this needs to include physical security, in order to prevent technical controls at the IT systems, applications and data level from being bypassed. This session covers the various areas to be addressed within the physical security domain.

- **Learning outcomes:**

The participant will gain a fuller understanding of how managing business continuity relates to physical security components within a BCM environment. Knowledge appertaining to the design-in-depth concept within the business continuity domain will be gained. Physical components that comprise physical security for data security, management and control will be fully understood in business continuity terms.

- **Lecture title:**

  Business Continuity Physical Security Part 2

- **Lecture description:**

This session builds upon the previous session, with an expansion of both the frames of reference, for how physical security plays a fundamental role in business continuity planning, as well as elements such as how to define requirements for a backup data center. These include electric supply, fire suppression systems, signage, physical access considerations, HVAC systems, as well as asset tracking and third-party assessment.

- **Module 9 Title:** 09. Business Continuity Physical Security Part 3
- **Description:**

When business continuity, recovery and reinstatement of systems and data are discussed, there is a general line of thought of the more technological aspects to maintaining resilience through redundancy, offsite backups, and so forth. However, this needs to include physical security, in order to prevent technical controls at the IT systems, applications and data level from being bypassed. This session covers the various areas to be addressed within the physical security domain.

- **Learning outcomes:**

The participant will gain a fuller understanding of how managing business continuity relates to physical security components within a BCM environment. Knowledge appertaining to the design-in-depth concept within the business continuity domain will be gained. Physical components that comprise physical security for data security, management and control will be fully understood in business continuity terms.

- **Lecture title:**

  Business Continuity Physical Security Part 3

- **Lecture description:**

This final session within the physical security and business continuity domain, expands in further detail on the various areas impacting upon BCM plan development. This includes site selection criteria for backup data centers, as well as definitions of sites. Additional information on power generation from backup supplies, electromagnetic interference, fire system components are disclosed.

- **Module 10 Title:** 10. Risk Management Via Risk Transfer

- **Description:**

Cyber risk management differentiates itself from cyber security through the use of non-technological forms of risk mitigation. The three options available within the risk management domain are to either accept, reject, or mitigate risks; the latter including risk transfer as a form of mitigation strategy available to organizations. There are technical, strategic and financial reasons as to why an entity may wish to utilize risk transfer as part of cyber risk management.

- **Learning outcomes:**

The participant will gain an insight into the multiple factors that are required to be assessed as part of the cyber risk management mitigation function within organizations, including the means by which transfer is achieved. They will also comprehend the issues in relation to the various options available to all entities, whether from a technical, or financial perspective. A

fuller understanding of the use of financial instruments and how they are playing an increasingly important role in transferring cyber risk financial exposure will also be attained.

- **Lecture title:**

  Risk Management Via Risk Transfer Part 1

- **Lecture description:**

This session covers the rationale and issues relating to the use of risk transfer for technological, strategic and financial objectives within an entity. It discloses the problems arising from triggering events, valuation, third-party validation and limitations related to the use of this form of cyber risk management strategy. Coverage relating to non-tangible assets, cost-benefit analysis for IT implementations versus third-party technology transfer, along with sectoral and organizational influences are discussed.

- **Module 10 Title:** 10. Risk Management Via Risk Transfer

- **Description:**

Cyber risk management differentiates itself from cyber security through the use of non-technological forms of risk mitigation. The three options available within the risk management domain are to either accept, reject, or mitigate risks; the latter including risk transfer as a form of mitigation strategy available to organizations. There are technical, strategic and financial reasons as to why an entity may wish to utilize risk transfer as part of cyber risk management.

- **Learning outcomes:**

The participant will gain an insight into the multiple factors that are required to be assessed as part of the cyber risk management mitigation function within organizations, including the means by which transfer is achieved. They will also comprehend the issues in relation to the various options available to all entities, whether from a technical, or financial perspective. A fuller understanding of the use of financial instruments and how they are playing an increasingly important role in transferring cyber risk financial exposure will also be attained.

- **Lecture title:**

  Risk Management Via Risk Transfer Part 2

- **Lecture description:**

The attendee is introduced to reinsurance concepts, together with the options for using insurance linked securities for cyber risk exposure transfers. Vehicles such as captives, cyber CAT bonds, and sidecars are covered, along with the relevant structures, costs and compliance issues. This is allied to explanations of how the cyber exposure gap may be filled is also explained without recourse to re/insurance industry knowledge being required. The session closes with looking at blockchain technologies as a form of transferred processing integrity as an option for future usage, including smart contracts.

- **Module 11 Title:** 11. Managing Cloud Security
- **Description:**

Cloud computing has undergone rapid adoption as a result of the urgent need to continue organizational operations during the Covid-19 pandemic. This resulted in personnel having to work remotely, whilst maintaining concurrent process and relationship integrity, requiring wholescale cloud migrations to third party vendors. Prior infrastructure and topologies

required similar skill sets, but cloud requires additional ones that remain lacking in availability on a global basis. This has placed entities in the invidious position of relying upon cloud service providers and third-party cloud-specific cloud security providers. Managing the risks arising from mainstream cloud usage requires organizations to reassess how they manage their cloud cyber security from technical and organizational perspectives.

- **Learning outcomes:**

The participant will comprehend the various elements that comprise managing identities, authentication and the requisites for accountability, both within and external to a cloud environment. Insight into the differences and consequences for cyber security control auditing in on-premise, cloud and hybrid topologies will be attained. The critical aspects of access control, including authentication protocols, single sign-on, provisioning lifecycle management and active directory will be understood for both cloud and non-cloud environments.

- **Lecture title:**

  Managing Cloud Security Part 1

- **Lecture description:**

The attendee is introduced to identity and access management as a general principle that can then be applied within the cloud security domain, due to this being a critical area for maintaining cyber security operation and remains the main cause of cloud breaches. The session introduces the concepts of identification, authentication, access and accountability, along with recapping authentication from elsewhere within this course. Authentication protocols and changes to auditing to encompass the changes made by cloud use are discussed.

- **Module 11 Title:** 11. Managing Cloud Security
- **Description:**

Cloud computing has undergone rapid adoption as a result of the urgent need to continue organizational operations during the Covid-19 pandemic. This resulted in personnel having to work remotely, whilst maintaining concurrent process and relationship integrity, requiring wholescale cloud migrations to third party vendors. Prior infrastructure and topologies required similar skill sets, but cloud requires additional ones that remain lacking in availability on a global basis. This has placed entities in the invidious position of relying upon cloud service providers and third-party cloud-specific cloud security providers. Managing the risks arising from mainstream cloud usage requires organizations to reassess how they manage their cloud cyber security from technical and organizational perspectives.

- **Learning outcomes:**

The participant will develop an understanding of how cloud identity and access management function, with comprehension of the concepts of single sign-on and federated identity. The risk versus workload and human error risks will be understood, along with how to manage such risks through the adoption of best practice within cloud environments. Attendees will learn how the different platforms methods of user and service provisioning are utilized and managed. Account types, and the use of groups for cloud user management will be comprehended, as well as the types of attacks most common within cloud computing.

- **Lecture title:**

  Managing Cloud Security Part 2

- **Lecture description:**

The participants are shown the various types of services that are offered by cloud vendors and how the topology of cloud environments are structured and function. The risks and impacts upon the CIA triad are disclosed, coupled to learning how third-party compromises can arise from cloud utilization. Identity and access management within the cloud are explained, along with the various modes of authentication for the three largest cloud platforms. An overview of the different management consoles from each of the major providers is given so that attendees can comprehend how these may differ in their functionalities and user interfaces.

- **Module 12 Title:** 12. Business Continuity & Incident Response
- **Description:**

Module 9 covers business continuity in the context of physical security. This session discloses the three pillars of business continuity planning, incident response planning and disaster recovery planning, in the context of an entity's IT systems and data. Areas covered include both technical and organizational aspects related to maintaining continuity of services to enable organizations to function following the impact of an adverse event.

- **Learning outcomes:**

The participant will gain an understanding of the relationship and differences between Business Continuity Planning, Incident Response Planning and Disaster Recovery Planning. Knowledge will be attained of what elements are required within the three types of plans. The fundamental requirements for hardware, software and data in the context of the CIA triad, with the focus being upon availability, allied to integrity are disclosed.

- **Lecture title:**

  Business Continuity & Incident Response

- **Lecture description:**

This module covers the principles and best practice for the maintenance of IT services for an organization. What components of continuity plans are required, which options are available to every organization are explained and why certain mitigating controls may not be utilized. Which teams undertake which roles in the case of an impacting event, whether technological, natural or environmental is illustrated. The regulatory environment and how it impacts upon BCM strategies is illustrated.

- **Module 13 Title:** 13. DEVOPS & SYSTEM SECURITY
- **Description:**

This session explains how various technical and non-technical elements are utilized in securing daily operations. Types of monitoring and logging, along with digital forensics and regulatory compliance tools are illustrated. The tools and systems available for acquiring, analyzing and utilizing various forms of threat intelligence data are described, along with changes as a result of AI and large language model use.

- **Learning outcomes:**

The participant will comprehend SIEM, SOAR and XDR systems, their differences and their applicability according to security domains. Concepts such as systems and software hardening will be learned, allied to applicable NIST and CIS frameworks for hardening. Both

technical and organizational contributing components in securing, such as patch and change management, visualization, drill-down tools, and honeypots will be understood.

- **Lecture title:**

  DevOps and System Security

- **Lecture description:**

This module covers the concepts of threat data use across various pillars of securing an organizations' normal operational mode, ranging from its' use within IT solutions, to organizational group composition for change management, as well as how the current and evolving regulatory environment requires entities to adopt such use for compliance. The use of digital forensics and its application for legal proceedings is disclosed. An explanation of the variances and requirements of technological systems in generating automated security responses is provided.

- **Module 14 Title:** 14. DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 1
- **Description:**

This session explains the concept of Zero Trust Computing from both a technical and organizational perspective. The types of software code and programming languages are covered, along with the software development lifecycle. The principal development options, including differentiation between Agile, Scrum and Scaled Agile Frameworks are illustrated. Databases and the forms, allied to the languages utilized for their management is disclosed.

- **Learning outcomes:**

The participant will comprehend the various forms of software code; their advantages and disadvantages, as well as how they are utilized. Security through the Zero Trust Computing concept will be learned and the participants will understand the role of various NIST frameworks in relation to securing software during its development and what elements require addressing. A basic understanding of databases and the concept of integrity will be attained, enabling security principles and how they apply to relational databases will be gained.

- **Lecture title:**

DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 1

- **Lecture description:**

This module covers the concept of Zero Trust Computing and what this entails from both technical and organizational controls and management. What forms of software code, their application domains and the benefits of one type over another are discussed. Types of software released is explained, along with how to mitigate the risks of not accessing code. Databases and their formats are disclosed, along with the underpinning requisites for their operation, control and integrity. Database languages are explained, with the concept of integrity for databases and data control highlighted.

- **Module 14 Title:** 14. DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 2
- **Description:**

Participants are shown the different methods utilized in developing software, with a recap of those utilized within the project management domain and how they apply within the DevOps environment. The most common types of software vulnerability attacks are described in terms of their mode of operation and what areas within software mal-actors are targeting with such attacks.

- **Learning outcomes:**

The various methods of software development will be learned, including what tools developers use for the creation and changing of software applications. An understanding of how software attacks are undertaken and why software vulnerabilities exist will be gained. How exposures to software attacks may be mitigated within the development environment will be comprehended, from a software development perspective.

- **Lecture title:**

DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 2

- **Lecture description:**

This module covers the software development domain, ranging from the methods and processes involved, to which computer languages are less secure from software application attacks and why. How mal-actors execute software attacks is described, together with best practice for the reduction and mitigation of such software-targeted attacks. The most prevalent types of attack are explained, to provide a full comprehension of what developers must account for during the software development process.

- **Module 14 Title:** 14. DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 3

- **Description:**

This session discloses how external and internal data sources can assist in the creation of more secure software code and overall application resilience to common attacks. The most used sources for threat data and attack methods are explained, as well as how to utilize such data within the development environment. Maturity models are discussed, along with the method of selection for vendor-sourced applications and systems.

- **Learning outcomes:**

The participant will learn how publicly available data and internal log file data can be leveraged within the software development process to integrate security within code. Participants will understand the role of development methods in the creation of applications that are aligned with user expectations and business cases. The method of selection of vendors in the software acquisition process will be attained for broad case usage. The differences in software analysis methods will also be understood.

- **Lecture title:**

DEVOPS & SECURE SOFTWARE DEVELOPMENT PART 3

- **Lecture description:**

This module introduces the participant to software development methodologies and their management. The data sources relating to multiple facets of software and system design and development, ranging from threat data, to open-source code analysis tools are provided. The process by which software is selected for development or purchase across the 5 primary strands is explained. How to measure and maintain cyber threat resilience through maturity models and their applicability within different domains is discussed. How business

objectives and the positioning of security within such objectives, with decomposition methods to ensure alignment are explained.

- **Module Title:** Course Closure & Summary

- **Description:**

This concluding session reviews the overall course modules covered and includes a few summary points to ensure that participants are as prepared for certification as possible, together with guidance on self-study prior to registering for the GIAC GSLC examination. Included is information relating to the examination process, passing grade and summary points that have been covered within the course.

- **Learning outcomes:**

Participants will take away knowledge from this session on how best to prepare for taking the GSLC examination, including where to refer to for additional self-study materials, in order to have sufficient knowledge of the core subject areas to be able to pass the examination.

- **Lecture title:**

  Course Closure & Summary

- **Lecture description:**

This short summary session recaps the main curriculum areas covered in this course and provides a summary of what is required of participants to register and take the GSLC examination. It refers to the roadmap to taking the examination and maintaining certification.
