CMMC Mapping

Suggested SANS Courses and Certification

SANS | GIAC CERTIFICATIONS

DOMAIN	MISSION	COURSE/PRODUCT	GIAC CERTIFICATION
Awareness and Training	The objective of the awareness and training domain is to educate users on common security threats, security best practices, and security policies. Training covers both privileged and non-privileged users. Privileged users receive additional role-relevant training. Security awareness training is critical as it improves user resiliency against cyber-attacks particularly social engineering attacks and insider threats.	**Security Awareness Training** LDR433: **Managing Human Risk**	 SSAP **SANS Security Awareness Professional**
Executive Cyber Exercise	The exercise is designed to immerse senior leadership (C-suite, senior managers, support function leads, technical SMEs) into a simulated major cyber-incident scenario, placing them in the midst of a "crisis" and asking them to respond, make decisions, and manage the event.	**Cyber Crisis Exercise**	
Incident Response	The objective of the incident response domain is for companies to establish an incident response capability, to prepare for incidents, detect, analyze, contain, recover, document, and report incidents. This involves creating an incident response plan, creating an incident response team, and testing your incident response capabilities.	FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics** FOR572: **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**	GCFA **GIAC Certified Forensic Analyst** GNFA **GIAC Network Forensic Analyst**
Leadership	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.	LDR514: **Security Strategic Planning, Policy, and Leadership** LDR519: **Cybersecurity Risk Management and Compliance**	GSTRT **GIAC Strategic Planning, Policy, and Leadership**
Penetration Tester	The objective of the penetration tester domian is to assess the effectiveness of security controls, reveal and utilise cybersecurity vulnerabilities, and to assess their criticality if exploited by threat actors.	SEC504: **Hacker Tools, Techniques, and Incident Handling** SEC560: **Enterprise Penetration Testing**	GCIH **GIAC Certified Incident Handler** GPEN **GIAC Penetration Tester**
Access Control	The objective of the access control domain is to limit access to your systems and data. This includes limiting persons who can log into your systems, limiting system access to authorized devices, limiting permissions so that users, devices, and processes can only access the resources they need to fulfill mission requirements. Examples of access controls include account management, separation of duties, least privilege, and session locks.	SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**	GDSA **GIAC Defensible Security Architecture**
Audit and Accountability	The objective of the audit and accountability domain is to record system and security logs on systems to support the monitoring, investigation, and reporting of system activity. It also seeks to ensure that system audit logs can be traced back to users so that they can be held accountable for their actions.	SEC301: **Introduction to Cyber Security** SEC566: **Implementing and Auditing CIS Controls**	GISF **GIAC Information Security Fundamentals** GCCC **GIAC Critical Controls Certification**
Configuration Management	The objective of the configuration management domain is to ensure that information system components such as endpoints, network devices, cloud resources, and servers maintain secure configurations. This involves creating hardware and software inventories, creating secure baseline configurations, deploying secure baseline configurations, maintaining these baselines, and requiring information system changes to be tested and approved prior to deployment.	SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations** SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**	GSOC **GIAC Security Operations Certified** GDSA **GIAC Defensible Security Architecture**
Identification and Authentication	The objective of the identification and authentication domain is to verify the identity of users and devices before granting them access to your information system. This involves creating unique user and device identifiers such as user names and computer names, requiring the use of strong passwords and multifactor authentication.	SEC401: **Security Essentials – Network, Endpoint, and Cloud** SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**	GSEC **GIAC Security Essentials** GDSA **GIAC Defensible Security Architecture**
Maintenance	The objective of the maintenance domain is to ensure that organizations perform timely and authorized maintenance on their systems in accordance with best practices and in a manner that is conducive to security. Maintenance is performed on both hardware and software (e.g., operating systems). Maintenance involves performing preventative, corrective, and adaptive maintenance. The maintenance domain also covers the secure performance on maintenance.	SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations** SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**	GSOC **GIAC Security Operations Certified** GDSA **GIAC Defensible Security Architecture**
Media Protection	The objective of the media protection domain is to protect the data stored on both digital and non-digital media from unauthorized access. Digital media includes storage devices such as hard drives and thumb drives. Non-digital media includes paper work. Media is protected by using locked containers, encryption, and proper media disposal techniques.	SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations** SEC511: **Cybersecurity Engineering: Advanced Threat Detection and Monitoring**	GSOC **GIAC Security Operations Certified** GMON **GIAC Continuous Monitoring Certification**
Personnel Security	The goal of the personnel security domain is to minimize the risk staff pose to your assets. This includes the malicious use of their legitimate system access. Employees often have access to sensitive information. The personnel security domain seeks to ensure that your company hires trustworthy staff and follows established procedures when terminating or transferring staff.	LDR519: **Cybersecurity Risk Management and Compliance** SEC511: **Cybersecurity Engineering: Advanced Threat Detection and Monitoring**	 GMON **GIAC Continuous Monitoring Certification**
Physical Protection	The objective of the physical protection domain is to limit physical access to your facilities, systems, support infrastructure, and equipment to authorized persons. This is accomplished by using locked entrances, ID badges, security cameras, and visitor escort procedures.	LDR433: **Managing Human Risk** SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations**	SSAP **SANS Security Awareness Professional** GSOC **GIAC Security Operations Certified**
Risk Assessment	The objective of the risk assessment domain is for companies to identify, evaluate, and manage risk. It is unrealistic to eliminate all risk, however proper risk management reduces risk. Risks are identified by performing risk assessments and are documented in a risk assessment reposition.	LDR419: **Performing A Cybersecurity Risk Assessment** LDR519: **Cybersecurity Risk Management and Compliance**	
Security Assessment	The objective of the security assessment domain is for companies to periodically assess the implementation of their security practices to verify their effectiveness. Any ineffective or absent security practices are to be documented and mitigated at a later date. Security assessments often involve reviewing your system security plan.	SEC401: **Security Essentials – Network, Endpoint, and Cloud** SEC566: **Implementing and Auditing CIS Controls**	GSEC **GIAC Security Essentials** GCCC **GIAC Critical Controls Certification**
System and Communications Protection	The objective of the system and communications protection domain is to provide safeguards that protect systems as well as information at rest or in transit. This domain involves the implementation of network segmentation, encrypted communications, and configuration settings limiting the use of mobile code.	SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations** SEC510: **Cloud Security Engineering and Controls**	GSOC **GIAC Security Operations Certified** GPCS **GIAC Public Cloud Security**
System and Information Integrity	The objective of the system and information integrity domain it to assure that the information system is free of malicious code and that appropriate measures are in place to prevent the installation of malicious code. This generally involves the use of anti-malware software, intrusion detection and prevention systems, as well as vulnerability scanning.	FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** SEC503: **Network Monitoring and Threat Detection In-Depth**	GREM **GIAC Reverse Engineering Malware** GCIA **GIAC Certified Intrusion Analyst**