Appendix 2 – Glossary of Terms

Term	Definition
Advanced Persistent Threat	A set of structured continuous and sophisticated attacks that are used to compromise a targeted entity
Anomaly-based monitoring	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations
Authenticated Vulnerability Scanning	A scan that uses system credentials to discover vulnerabilities that may exist on an Information System
Authentication, Multi-factor	Authentication using two or more of the following factors: ➢ knowledge factor, 'something an individual knows'; ➢ possession factor, 'something an individual has'; ➢ biometric factor, 'something an individual is or is able to do'.
Authentication, Single-factor	Authentication using only one of the following factors: ➢ knowledge factor, 'something an individual knows'; ➢ possession factor, 'something an individual has'; ➢ biometric factor, 'something an individual is or is able to do'.
Authentication, Strong	Authentication using one of the following factors more than once before allowing access to the Information System: ➢ knowledge factor, 'something an individual knows'; ➢ possession factor, 'something an individual has'; ➢ biometric factor, 'something an individual is or is able to do'.
Cyber Event	An observable occurrence in an Information System
Cyber Incident	A cyber event that jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits
Cyber Threat Hunting	The process of proactively and iteratively searching the computing environment to detect and isolate threats that have evaded existing security controls
Distributed Denial of Service	A type of cyber attack where multiple compromised systems are used to make an Information System unavailable for its intended users
Indicators of Compromise	A piece(s) of forensic data that identifies potential malicious activity on an Information System
Information System	A set of applications, services, information technology assets or other information handling components
Key Performance Indicator	A measurement that gauges how well a service is performing against its goals
Key Risk Indicator	A measurement that is used to determine the level of risk to which an organization is exposed
Penetration Testing	The process of conducting real-world attacks against an Information System to identify security weaknesses before they are discovered and exploited by others
Phishing	A digital form of social engineering that uses authentic-looking - but bogus - e-mail to request information from users or direct them to fake websites that request information

Term	Definition
Ransomware	A type of malicious software that prevents or limits users from accessing their system either by locking the system screen or files until a ransom is paid
Spearphishing	A digital form of social engineering that uses an authentic-looking - but bogus - e-mail to request information from a distinctive set users (e.g. corporate executives) in an attempt to have them provide sensitive information
Tactics, Techniques and Procedures (TTP)	The behavior of a threat actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures are an even lower-level, highly detailed description in the context of a technique
Threat Actor	An individual, group, or organisation believed to be operating with malicious intent
Threat Intelligence	The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions and activities that offer courses of action to enhance decision making
Three Lines of Defense	A management risk control framework which consists of three levels used to provide oversight of an organization’s risks
Unauthenticated Vulnerability Scanning	A scan that attempts to discover vulnerabilities on an Information System through limited system access
Waterholing Attack	A security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit