| Top level category | Category Description | Subcategory | Item Description |
|---|---|---|---|
| Information Risk Assessment and Management | This includes companies that provide products or services that aid organisations with the business oriented side of cyber security, including regulatory, management and planning aspects. It includes the provision of support for IT Risk Assessment, security testing, secure data management, IT HR governance, and secure product development. | Regulatory Compliance | Organisations providing advisory, design and provision services or tools that aids a customer's cyber security compliance towards regulations such as GDPR, PCI and various government or professional standards, as well as ensuring contractual specifications are met. |
| | | Secure Data Management | Services or tools offered that focus on protecting the integrity of digital and non-digital data and ensuring its security both at rest and in transit. This includes Information Security tools and strategies to prevent, detect and respond to attacks on information, including the provision of chief information security officers (CISO) and chief information officers (CIO) for an organisation; as well as data confidentiality practices such as encryption, data destruction, metadata removal and shared repository security. |
| | | Secure Product Development | This category covers business solutions, products and services offered that provide guidance on a secure approach to hardware and software product development and DevOps in general, as well as the testing, assessment and training for the principles and good industry practices of the field. |
| | | Enterprise Security Management | Products or services that contribute to the creation and management of the corporate, enterprise aspects of cyber security/cyber security aspects of corporate governance. This can include topics such as  Auditing and Assurance, Policy and Configuration Management, Patch Management. |
| | | Employee Governance | Services or products offered that aid customers manage a holistic cyber-wise governance of employees. Activities covered can be monitoring, filtering and protecting their online activities and data, providing cyber security awareness training, but also security testing such as insider threat detection and social engineering/phishing experiments with the purpose of educating employees belongs here. |
| | | Security Testing and Risk Management | Products or services that carry out a form of testing of the company's cyber security policies, IT infrastructure, employees and processes to review and assess how these react to various cyber attacks and breaches. This can include (but is not limited to)  Security Scanning, Risk Assessment, Ethical hacking, Penetration Testing, Vulnerability Testing, Insider Threat Analysis, Security Product Quality Assurance and DDOS Simulation. |
| Identification, authentication and access control | Companies providing services or tools to control, plan and provision access to computer networks, by identifying and authorising the parties wishing to gain access. | Authentication | The provision of services, hardware or software products that focuses on the validation of users, processes or products. This category can include solutions such as digital, biometric, software or hardware/token-based authentication, password security products, physical document validation, and two-step and two-factor authentication. |
| | | Identity & Access Management | This category includes products or services offered by companies that ensures an effective and secure identification and authorisation to control access to ICT software or hardware components. This covers topics such as identity provisioning and management, password management, one-time or single sign-on, and identity security issues as identity theft. |
| Network Security | Companies that provide services or products that are designed to protect the usability and integrity of a network and its data, including both the hardware and software components of its core and non-core infrastructure. | Web Content Filtering | This category covers the high-level software aspects of network security management, with focus on preventative actions in relation to browsing experience, such as DNS protection, URL validation, Site blocking, VPN Services, as well as general Cloud security. |
| | | Secure Network Infrastructure | Companies offering products or services that include the securing of core and non-core network hardware infrastructure, peripherals and media, including Internet of Things (IoT) and embedded devices, and relevant software solutions required for them. |
| | | Systems Integrity | This category covers the software aspects of network security management with focus on the protection of the network as a whole. This includes enterprise security management practices, such as Firewall Management, Virtualisation, Secure Architecture/Platform Provision, Code injection and Packet Capture protection, SSL solutions, Transmission/Messaging encryption, eavesdropping and keylogging protection, as well as general device application security. |
| End-user device Security | Products or services offered that protect the end-user's online activities by localised safeguarding of their device and its processes, not via the network infrastructure. | Device Protection and Access Control | The provision of products or services that protect the network and end-user device integrity - this can include practices such as location- or reputation based trust management/device access control, as well as device IT security maintenance, including the provision of anti-virus software on devices, firewall settings management, etc. |
| | | Email & Messaging Security | Products and services offered that focus on the end-device communication security in the application layer, such as the archiving, retrieval, destruction and filtering of emails and other types of digital messages, the detection and management of compromised accounts, malicious messages; as well as protection against SPAMs, Phishing and Pharming. |
| Monitoring, Detection and Analysis | Products or services offered that monitor processes, tasks or the complete IT system of the customer; pro- or reactively scan for and detect threats and malicious activities; and analyse the course and effects of events. | Active Monitoring and Defence | Companies offering services or products that actively monitor and protect the client IT infrastructure for cyber security breaches. Can include activities such as dark web- and endpoint scanning, situational awareness, intrusion detection, malicious content alerting, etc. |
| | | Fraud & Transaction Security | Products and services that aid data integrity protection, document signature security and the emerging transaction and fraud protection focused technologies, such as blockchain and cryptocurrencies. |
| | | Adversary Analysis | Products or services that proactively analyse a variety of sources for threats, and usually provide reports on current global and company-focused adversary intelligence, including possible preventative actions to take. |

| | | | |
|---|---|---|---|
| | | Security Operations Centre (SOC) | This includes provisioning the development of an SOC for the customer, or offering a managed SOC and managed monitoring of the customer's systems. |
| Incident Response and Management | Companies providing services or products to prepare for, respond to and manage cyber security incidents, with focus on maintaining and recovering data and mission critical operations, plan and carry out reactions to security breaches, and gather and present digital evidence to analyse an event occurred. | Disaster Recovery | Companies offering a service or products that aid the setting and maintenance of policies and procedures to ensure that in the event of a natural or human-induced disaster critical technology infrastructure and other vital support systems are restored to normal in as short time as possible and the company can quickly resume mission critical functions afterwards. |
| | | Business Continuity Services | Companies offering services or tools to design, provision, test and maintain company business continuity plans that ensure that in the case of a large-scale negative event an organisation can maintain operations throughout. |
| | | Backup Provision and Management | Providing tools or services to plan and maintain backups of business data or IT infrastructure. |
| | | Breach Response | Tools and services offered that focus on responding to ongoing or past security incidents. This can include, but is not limited to reactive responses such as counter-attacks, event scale remediation, as well as  proactive measures such as employee tabletop exercises, incident response plan provision, etc. |
| | | Vulnerability Management | The management of currently existing or possibly occurring cyber security vulnerabilities in the customer infrastructure, including the triaging of said hazards and the detailing of preventative and reactive actions to be taken in the case of incidents. Also, in a somewhat of an overlap with Breach Response, covers general post-incident investigation for security revision purposes. |
| | | Forensics | Companies offering forensic service or tools that helps gather, process, interpret and preserve digital evidence relating to a possible breach in cyber security, that, if necessary can be used in the court of law. |
| SCADA and Information Control Systems: | This category includes the provision of secure control systems that are to be used in either Critical National Infrastructure facilities or industrial setting. These require higher security standards to be certified against, and can include the provision of only certain hardware or software components, or the overall system, as well as advisory, testing and certification services. | Critical National Infrastructure | Companies that provide services or products that are certified to be used for and in the IT systems of CNI facilities and sites, to protect and prepare them for cyber security events. |
| | | SCADA and ICS Provision and Compliance | Companies providing services to design, provision, maintain or certify software/hardware components or the complete system that can be used in Supervisory Control and Data Acquisition (SCADA) Systems and Industrial Control Systems (ICS). |
| Training, Awareness and Education | Organisations that provide products or services in relation to cyber security training, awareness or education | Cyber Security Training | Providing an awareness-level cyber security training to employees, to create a cyber security centered workplace environment and to educate employees on possible cyber security issues. Courses with the main focus on instilling good security practices in employees in order to prevent intruder access to the company's networks through human errors. |
| | | Corporate Cyber Security Training | Providing cyber security training to employees in a professional or certifiable manner, which goes beyond an awareness of cyber security issues at the workplace, to educate and train employees to implement measures to avoid a compromise on an individual and corporate level. This includes Cyber Essentials and Cyber Essentials Plus trainings, and other professional certifications. |
| | | Higher education and research | Providing higher education courses and conducting research in cyber security |
| Cyber Professional Services | Organisations that offer consultancy in a range of cyber security matters, and offer a holistic approach. | Cyber Security Consultancy | Companies that provide professional or consultancy services (e.g. advice or implementation of solutions) that focus on cyber security, and ones that provide services across a large number of other categories. |
| | | Certified Cyber Professional Services | NCSC Certified Cyber Consultancies are such which have demonstrated to NCSC that they have:<br>- A proven track record of delivering defined cyber security consultancy services<br>- A level of cyber security expertise supported by professional requirements defined by NCSC<br>- The relevant Certified Professional (CCP) qualifications<br>- Manage consultancy engagements in accordance with industry good practice<br>- Meet NCSC requirements for certified professional cyber services companies |