LECS REFERENCE, COMPLIANCE AND CERTIFICATION SUPPORT TABLE
Q1/2022

NIS

The EU Directive on Security of Network and Information Systems (NIS Directive) The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The NIS Directive applies primarily to Operators of Essentials Services (OES) that are identified by EU Member States and Digital Services Providers (DSP) that offer key digital services to persons within the EU. The NIS Directive entered into force in August 2016. EU member states – including the UK –were required to transpose the NIS Directive into their national laws by 9 May 2018 and must identify Operators of Essential Services by 9 November 2018.and sub-contractors of federal agencies that store, transmit, or manage CUI. This document is based on the Federal Information Security Management Act of 2002 (FISMA) Moderate level requirements. It went into full effect on December 31, 2017.

CATEGORY	**SUBCATEGORY**	**LECS TECHNOLOGY or LECS SOC Service**	**HOW IT HELP**
A.4 Supply chain	Network controls. Networks shall be managed and controlled to protect information in systems and applications	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	LECS SOC Service provide software and hardware necessary to compliance with security policy. LECS device/SaaS, in the specific case, can monitoring the network data flow to find any anomalies or security risk can encounter.
B.4 System security	Controls against malware Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	LECS SOC Service provide software and hardware necessary to compliance with system security policy. LECS device/SaaS, in the specific case, can monitoring the network data flow to find any anomalies or security risk can encounter, included the malware or exploit, shellcode etc..

	Network controls Networks shall be managed and controlled to protect information in systems and applications.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	LECS SOC Service provide software and hardware necessary to compliance with security policy. LECS device/SaaS, in the specific case, can monitoring the network data flow to find any anomalies or security risk can encounter.
B.6 Staff awareness and training	Security skills assessment Assessment of security skills and addressing skills gaps with appropriate training	LECS Service - Training	The Training service provide 3 level of training, based on the specific final user. From anti-phishing technique, to advanced policy for sys admin.
C.1 Security monitoring	System monitoring and control Tracking suspicious user activity and enabling instant incident response	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	LECS SOC Service provide software and hardware necessary to compliance with security policy. LECS device/SaaS, in the specific case, can monitoring the network data flow to find any anomalies or security risk can encounter. Further, the LECS automatically respond to isolate the threat in a air-gap way.
C.2 Proactive security event discovery	Proactively identify events and incidents Anomalous events in network and information systems are detected.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	The LECS device has an engine that constantly monitors the traffic it encounters, and works to detect network malware and infections that are proliferating. The SOC Service adds further human-skill review and analysis of LECS LOG and many more.
D.2 Lessons learned	Build resilient systems Continual improvement by assessing events and incidents, and analyzing	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	The SOC service and the LECS device toghether provide an optiaml component in user defence-chain.

	what has worked and what has not.		Operation as backup redundancy, or policy implementing are integrated in all services. Also, the Tiresia engine provide cloud support with ML engine to preview and mitigate the network threat.