IL7 and 27K1 – Facilitating Compliance with PCI DSS v4

IL7 is pleased to announce its partnership with 27K1. As transport cyber risk and compliance specialists, Il7 recognises the importance of security to safety and performance. Il7 has twenty years' experience working with transport companies, central government and MOD in risk management and compliance with NIST (new JSP 440/604 for MOD), GDPR (HMG) and NIS (Govia Thameslink). In the 20 years we have assisted all clients in aligning and / or complying with ISO 27001. Most recently with GTR we have worked with 27K1 who provided the easy-to-use compliance software tooling. Having worked with Banks (HSBC/Capital One) Il7 has always recognised the compliance needs of SOX and PCI DSS but never had time to develop the expertise in these fields. Transport companies also need to comply with these security regulations – they handle vast amounts of payment card details and on-line transactions and compliance can create a major overhead. Therefore, we see our partnership with 27K1 as being one of substantial purpose to the industry.

Visiting DTX, IL7 were staggered by the interest shown in 27K1 compliance software solutions. The quality of prospective customers and quantity of leads generated exceeded the expectations of company founders, Peter Farrer and Jeremy Martin. DTX provided a platform to launch the 27k1 Hybrid Software, which enables compliance to both ISO 27001 and PCI DSS V4.0.

March 31st, 2022, saw the Payment Card Industry - Security Standards Council release version 4.0 of its PCI Data Security Standard. This upgrade from Version 3.2.1 brings a raft of sweeping changes that provide a more innovative and safe approach for cardholders and their PAN – Personal Account Number data. For those companies that manage high volumes of financial transactions using credit cards and on-line payment systems, compliance is essential. Non-compliance, system breaches and data corruption within a merchant organisation carries the threat of sanctions or expulsion from the credit card provider. PCI DSS V4.0 offers 280 controls across 12 Requirements including 30 in Appendix A. These measures will strengthen security in the payment industry, ensuring rigid protocols against phishing, cybercrime and digital theft.

PCI DSS 4.0 will expand the cardholder data validation methodologies, delivering a safe payment experience in offline and online modes to the cardholders. It is a major improvement from Version 3.2.1, yet compliance will be increasingly complex, requiring strict attention to detail and sharp focus on data submission. Merchants that engage in online trade or that provide digital payment solutions to their customers are required to prove their compliance through self-assessment or audit by an external Qualified Security Assessor (QSA) who files their RoC – Report on Compliance to the organization's acquiring banks to demonstrate their compliance.

There are 9 different SAQ's – Self-Assessment Questionnaires. A company must select the applicable SAQ(s) to match their trading practices. 8 of these SAQ's are for Merchants and 1 - SAQ D, is for Service providers. SAQ A is the shortest with only 29 control requirements that need to elicit accurate responses. SAQ D has 260 similar control requirements for Service Providers. A Customised Approach allows the use of approved, alternative controls which like the regular controls, must be tested using a targeted risk analysis that is detailed, documented, and maintained. As risk and compliance practitioners, IL7 can resource, using 27K1 software such targeted risk analysis.

Because each customized implementation will be different, there are no defined testing procedures. Here, the assessor is required to derive testing procedures that are appropriate to the specific implementation to validate that the implemented controls meet the stated objective. The customised approach supports innovation in security practices, allowing entities greater flexibility to show how their current security controls meet PCI DSS objectives. This approach is intended for risk-mature entities that demonstrate a robust risk-management approach to security, including, but not limited to, a dedicated risk-management department or an organisation-wide risk management approach. Different Merchants, Different Rules!

Going further, Level 1 Merchants - those that process over 6 million debit or credit card transactions per annum, are required to undergo an ASV scan from an Approved Scanning Vendor every 3 months. This is intended to ensure that systems are secure. Additionally, Level 1 Merchants must access audit services from QSA's – who file an AOC – Attestation of Compliance on behalf of the Merchant, leading to the filing of the RoC. This is the only level that requires an on-site PCI DSS audit every year. Therefore, becoming PCI compliant often takes longer for Level 1 merchants. Level 2 Merchants process between 1 – 6 million card transactions per annum. They must complete the SAQ(s), perform a quarterly ASV network scan and complete the AOC. They may also require a QSA audit. The requirements of PCI Level 3 and 4 merchants that process fewer transactions remain highly structured and require completion of appropriate SAQ(s), but are marginally less stringent than the higher Levels. Conclusion: Under PCI DSS V4.0, compliance is going to be more complicated and resource heavy, completion of SAQ's will be prone to error by using spreadsheets and similar compliance tools.

The 27k1 Hybrid software will readily support compliance to PCI DSS version 4.0. Once the company has identified the appropriate SAQ(s) the 27k1 Hybrid software automatically offers the correct control requirements and auto-populates key responses, allowing the company to readily complete the SAQ in readiness for return to the PCI SSC.977.