		E4		WPNG	
Ques. Num	**Question**	**Response**	**Additional Information**	**Response**	**Additional Information**
SIG 2017 Lite					
SL.1	SL.1 Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? if yes, does it include:	**Yes**		**Yes - but**	Canvas has a process. Wiley has a process that may need tailoring for next gen
SL.2	SL.2 Is there a program to manage the treatment of risks identified during assessments?	**Yes**		**Yes**	
SL.3	SL.3 A formal process for assigning appropriate management ownership for each risk?	**No**		**No**	We do assign risk to implementers
SL.4	SL.4 A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?	**Yes**		**Yes**	
SL.5	SL.5 A formal process for tracking the status of action plans and reporting them to management?	**No**		**Yes**	Project and product managers are fully informed
SL.6	SL.6 Controls identified for each material risk?	**No**		**Yes - but**	Implement mitigation strategies and notifications via tech support among other things
SL.7	SL.7 Measures for defining, monitoring, and reporting risk metrics?	**No**		**Yes**	We do pen tests regularly plus on demand, manual code reviews, unit tests, monitoring tech support
SL.8	SL.8 Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there:	**Yes**		**Yes**	Procurement Team
SL.9	SL.9 A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:	**No**		**No**	
SL.10	SL.10 Approval by management?	**No**		**No**	
SL.11	SL.11 Annual review?	**No**		**No**	
SL.12	SL.12 Required reassessment when service delivery or contract changes?	**No**		**No**	
SL.13	SL.13 Review of the subcontractor's vendor management policy and procedures?	**No**		**No**	
SL.14	SL.14 Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?	**No**		**No**	
SL.15	SL.15 Is there a vendor management program?	**No**		**No**	Procurement
SL.16	SL.16 Do external parties have access to Scoped Systems and Data or processing facilities?	**Yes**		**Yes**	
SL.17	SL.17 Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?	**No**		**No**	
SL.18	SL.18 Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.	**No**		**Yes**	
SL.19	SL.19 Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?	**No**		**No**	
SL.20	SL.20 Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?	**No**		**Yes**	

SL.21	SL.21 Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?	**No**		**No**	
SL.22	SL.22 Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?	**No**		**No**	
SL.23	SL.23 Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	**Yes**	Table of Contents and Executive Summary will be provided.	**Yes**	
SL.24	SL.24 Have the policies been reviewed in the last 12 months?	**Yes**		**Yes**	
SL.25	SL.25 Is there a respondent information security function responsible for security initiatives?	**Yes**		**Yes**	
SL.26	SL.26 Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?	**Yes**		**Yes**	
SL.27	SL.27 Is information classified?	**No**		**No**	
SL.28	SL.28 Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?	**No**	We protect the endpoints with removable media and sensitive data is encrypted	**No**	We protect the endpoints with removable media and sensitive data is encrypted
SL.29	SL.29 Is Scoped Data sent or received via physical media?	**No**		**No**	
SL.30	SL.30 Are encryption tools managed and maintained for Scoped Data? If yes:	**No**	Wileyplus data in transport is encrypted using TLS, data at rest is not encrypted. Compensating controls are in place.	**yes**	All data traffic in and out of Canvas is encrypted using TLS, forward-secrecy-compliant ciphers whenever possible (e.g. ECDHE-ECDSA-AES128-GCM-SHA256). The acceptable cipher list is constantly maintained to ensure that no vulnerabilities are present (e.g. POODLE).
SL.31	SL.31 Are clients provided with the ability to generate a unique encryption key?	**No**		**No**	
SL.32	SL.32 Are clients provided with the ability to rotate their encryption key on a scheduled basis?	**No**		**No**	
SL.33	SL.33 Are staff able to access client Scoped Data in an unencrypted state?	**Yes**		**Yes**	
SL.34	SL.34 Are staff able to access client's encryption keys?	**No**		**No**	
SL.35	SL.35 Is data segmentation and separation capability between clients provided?	**Yes**		**Yes**	
SL.36	SL.36 Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other clients data if using resource pooling?	**No**		**Yes**	Sub accounts are created for each institution in order to segment data
SL.37	SL.37 Is there a data classification retention program that identifies the data types that require additional management and governance?	**No**		**No**	
SL.38	SL.38 Is there a self-service portal or API call available to clients which provides the ability to place a "Legal hold" on client data which may be subject to a legal action, without impacting other clients data retention or destruction schedules?	**No**		**No**	
SL.39	SL.39 Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include:	**Yes**		**Yes**	
SL.40	SL.40 Security roles and responsibilities?	**Yes**		**Yes**	

SL.41	SL.41 Background screening?	**Yes**		**Yes**	
SL.42	SL.42 Employment agreements?	**Yes**		**Yes**	
SL.43	SL.43 Security awareness training?	**Yes**		**Yes**	
SL.44	SL.44 Disciplinary process for non-compliance?	**Yes**		**Yes**	
SL.45	SL.45 Termination or change of status process?	**Yes**		**Yes**	
SL.46	SL.46 Are background checks performed for Service Provider Contractors and Subcontractors?	**Yes**		**Yes**	
SL.47	SL.47 Do information security personnel have professional security certifications?	**Yes**		**Yes**	
SL.48	SL.48 Is there a physical security program?	**No**	3rd party data centers have physical security measures in place	**Yes**	
SL.49	SL.49 Are physical security and environmental controls in the data center and office buildings?	**Yes**	Physical & logical access to our data-centers are restricted to a select few personnel, and they in turn have procedures to ensure that these are inaccessible by other personnel in the building. Access beyond Reception is secured by badge readers and video cameras. The data center is further secured by badge readers enabling access to an authorized subset of Technology staff.	**Yes**	AWS data centers utilize state-of-the-art electronic sureillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards and access is authorized strictly on a least-privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Multiple geographic regions and Availability Zones provide resilience in the face of most failure modes including natural disasters or system failures.
SL.50	SL.50 Are visitors permitted in the facility?	**Yes**	The following requirements are in place for all visitors coming into sensitive facilities (where target data is stored, processed or viewed): - All visitors signed in / logged - All visitors required to provide government issued ID - All visitors escorted at all times and required to wear clearly identifiable visitor credentials	**No**	Hosted at AWS
SL.51	SL.51 Are management approved operating procedures utilized?	**Yes**		**Yes**	
SL.52	SL.52 Is there an operational change management/change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	**Yes**		**Yes**	

SL.53	SL.53 Are backups of Scoped Systems and Data performed?	**Yes**	WileyPLUS database is configured with Oracle Data Guard (Primary database and Standby database) which is a high availability solution. The standby database is running RMAN backup weekly using Virtual Tape Library (data is backed up to Hitachi storage).	**Yes**	
SL.54	SL.54 Are Cloud Services provided? If yes, what service model is provided (select all that apply):	**No**		**Yes**	Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. Explore how millions of customers are currently leveraging AWS cloud products and solutions to build sophisticated applications with increased flexibility, scalability and reliability.
SL.55	SL.55 Software as a Service (SaaS)?			**Yes**	
SL.56	SL.56 Infrastructure as a Service (IaaS)?			**Yes**	
SL.57	SL.57 Private cloud?			**Yes**	
SL.58	SL.58 Public cloud?			**No**	
SL.59	SL.59 Community cloud?			**No**	
SL.60	SL.60 Hybrid cloud?			**Yes**	
SL.61	SL.61 Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?	**Yes**		**Yes**	
SL.62	SL.62 Are application self service features or an Internet accessible self-service portal available to clients?	**Yes**		**Yes**	
SL.63	SL.63 Can clients run their own security services within their own cloud environment?	**N/A**	Cloud environment N/A.	**No**	
SL.64	SL.64 Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?	**Yes**		**Yes**	
SL.65	SL.65 Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method:	**Yes**		**Yes**	Email, system annoucnements, Status page, Rep outreach
SL.66	SL.66 Is there a scheduled maintenance window? If yes, what is the frequency:	**No**		**No**	
SL.67	SL.67 Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime:	**No**		**No**	
SL.68	SL.68 Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated:	**Yes**	Status Page	**Yes**	Status Page. status.wileyplus.com
SL.69	SL.69 Are electronic systems used to transmit, process or store Scoped Systems and Data?	**Yes**		**Yes**	

SL.70	SL.70 Are individual IDs required for user authentication to applications, operating systems, databases and network devices?	**Yes**		**Yes**	
SL.71	SL.71 Are passwords used?	**Yes**		**Yes**	
SL.72	SL.72 Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms?	**Yes**		**Yes**	
SL.73	SL.73 Is remote access permitted?	**Yes**		**Yes**	
SL.74	SL.74 Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?	**No**		**No**	Next Gen will use CAS (Central Authentication System)
SL.75	SL.75 Is two factor authentication required to access the production environment containing Scoped Data?	**No**	Currently, there is no requirement for 2-factor authentication however, a user must be added in the to AD group in order to use a Wiley Wireless AP.	**No**	
SL.76	SL.76 Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this.	**No**		**Yes**	There are security policies in place to protect the user
SL.77	SL.77 Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?	**No**		**No**	There are security & privacy policies in place to protect the user
SL.78	SL.78 Are applications used to transmit, process or store Scoped Data?	**Yes**		**yes**	
SL.79	SL.79 Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?	**Yes**		**Yes**	
SL.80	SL.80 Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:	**Yes**		**Yes**	
SL.81	SL.81 Is HTTPS enabled for all web pages used as part of the scoped service?	**Yes**		**Yes**	
SL.82	SL.82 All available high-risk security patches applied and verified at least monthly?	**No**		**No**	*check canvas documentation
SL.83	SL.83 Are third party alert services used to keep up to date with the latest vulnerabilities?	**Yes**		**Yes**	
SL.84	SL.84 Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	**Yes**		**Yes**	
SL.85	SL.85 Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	**Yes**	Real time alerts, malware detection, threat intelligence - all cloud based.	**Yes**	
SL.86	SL.86 Is application development performed?	**Yes**		**Yes**	
SL.87	SL.87 Is there a secure software development lifecycle policy (including mobile software applications) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	**Yes**		**Yes**	
SL.88	SL.88 Is development, test, and staging environment separate from the production environment? If so, how are they segmented:	**Yes**	Production environments are segregated.	**Yes**	
SL.89	SL.89 Is there a formal Software Development Life Cycle (SDLC) process?	**Yes**		**Yes**	
SL.90	SL.90 Are change control procedures required for all changes to the production environment?	**Yes**		**Yes**	
SL.91	SL.91 Is Scoped Systems and Data ever used in the test, development, or QA environments? If yes, is:	**Yes**		**Yes**	

SL.92	SL.92 Is there a documented change management / change control process? If yes, does it include:	Yes		Yes	
SL.93	SL.93 Are compilers, editors or other development tools present in the production environment?	Yes			
SL.94	SL.94 Is a secure code review performed at least annually?	Yes		Yes	
SL.95	SL.95 Is each release subject to a full secure code review?	Yes		Yes	
SL.96	SL.96 Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?	Yes	Business critical applications are subject to penetration testing as needed.	Yes	
SL.97	SL.97 Is there a formal development methodology in operation? If yes, which groups does it include?:	Yes		Yes	Product Management, SQA, Development, Project Management
SL.98	SL.98 Are mobile applications that access Scoped Systems and Data developed?	No		Yes	
SL.99	SL.99 Is there an Incident Management Program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does the program include:	Yes		Yes	
SL.100	SL.100 Privacy Incidents?		*ask Robyn about e4 response		
SL.101	SL.101 Is there a formal Incident Response Plan?	Yes	Wiley has a documented incident response plan and will alert in compliance with international data protection legislation.	Yes	
SL.102	SL.102 Is there a 24x7x365 staffed phone number available to clients to report security incidents?	Yes	Customers can contact Technical Support at: https://hub.wiley.com/community/support/wileyplus	Yes	
SL.103	SL.103 Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?	Yes		Yes	
SL.104	SL.104 Has a Business Impact Analysis been conducted?	No		No	
SL.105	SL.105 Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?	No		No	
SL.106	SL.106 Are specific response and recovery strategies defined for the prioritized activities?	No			
SL.107	SL.107 Are formal business continuity procedures developed and documented?	No		No	
SL.108	SL.108 Has senior management assigned the responsibility for the overall management of the response and recovery efforts?	Yes		Yes	
SL.109	SL.109 Is there a periodic (at least annual) review of your Business Resiliency Program?	Yes		Yes	
SL.110	SL.110 Are there any dependencies on critical third party service providers?	Yes		Yes	
SL.111	SL.111 Is there a formal, documented exercise and testing program in place?	No		Yes	
SL.112	SL.112 Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?	No		No	
SL.113	SL.113 Is there a specific Recovery Time Objective (RTO)? If yes, what is it?	No		No	
SL.114	SL.114 Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?	No		No	
SL.115	SL.115 Are site failover tests performed at least annually?	No		No	

SL.116	SL.116 Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?	**Yes**		**Yes**	
SL.117	SL.117 Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?	**Yes**		**Yes**	
SL.118	SL.118 Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?	**Yes**		**Yes**	
SL.119	SL.119 Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?	**Yes**		**Yes**	
SL.120	SL.120 Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?	**Yes**		**Yes**	
SL.121	SL.121 Is licensing maintained in all jurisdictions where required?	**Yes**		**Yes**	
SL.122	SL.122 Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?	**Yes**		**Yes**	
SL.123	SL.123 Are marketing or selling activities conducted directly to Client's customers?	**No**		**No**	
SL.124	SL.124 Are there direct interactions with your client's customers?	**Yes**		**Yes**	
SL.125	SL.125 Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?	**Yes**		**Yes**	
SL.126	SL.126 Is there a documented governance process to identify and assess changes that could significantly affect the system of internal controls for security, confidentiality and availability?	**Yes**		**Yes**	
SL.127	SL.127 Are accounts opened, transactions initiated or other account initiation activity applying payments, taking payments, transferring funds, etc. through either electronic, telephonic, written or in-person requests made on behalf of your client's?	**No**		**No**	
SL.128	SL.128 Are these sites, applications and systems used to also transmit, process or store non-scoped data?	**No**		**No**	
SL.129	SL.129 Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?	**Yes**		**Yes**	
SL.130	SL.130 Does the service provider permit client audits and assessments?	**No**		**No**	
SL.131	SL.131 Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:	**Yes**		**Yes**	

SL.132	SL.132 Security configuration standards documented? If yes, are:	**No**	There are standard build and patching requirements however, no written documentation exists. We are in the process of implementing policies and procedures based on NIST.	**Yes**	We have written documentation for Canvas
SL.133	SL.133 All available high-risk security patches applied and verified at least monthly on all server platforms?	**No**		**No**	
SL.134	SL.134 Sufficient detail contained in Operating System and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?	**Yes**		**Yes**	
SL.135	SL.135 Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	**Yes**		**Yes**	
SL.136	SL.136 Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:	**No**		**No**	
SL.137	SL.137 View Scoped Data?				
SL.138	SL.138 Process Scoped Data?				
SL.139	SL.139 Delete Scoped Data?				
SL.140	SL.140 Store Scoped Data?				
SL.141	SL.141 Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?	**No**		**No**	
SL.142	SL.142 Is there a Mobile Device Management solution in place?			**No**	
SL.143	SL.143 Is there an approved process for IT to off-board mobile devices when a constituent terminates, or requests to on-board a new mobile device? If yes, does it:				
SL.144	SL.144 Are staff technically prevented from accessing the administrative environment via non-managed private devices? If yes, is it from:	**Yes**		**Yes**	
SL.145	SL.145 Are there external network connections (Internet, extranet, etc.)?	**Yes**		**Yes**	
SL.146	SL.146 Security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?	**Yes**	Wiley security standards document will be provided	**Yes**	
SL.147	SL.147 Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?	**Yes**		**Yes**	
SL.148	SL.148 Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?	**Yes**		**Yes**	
SL.149	SL.149 Are all available high-risk security patches applied and verified at least monthly?	**No**		**Yes**	
SL.150	SL.150 Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are enabled?	**Yes**		**Yes**	
SL.151	SL.151 Are wireless networking devices connected to networks containing scoped systems and data?	**Yes**		**Yes**	

SL.152	SL.152 Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?	**No**		**Yes**	
SL.153	SL.153 Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data.	**Yes**	WileyPLUS is fully compliant with FERPA (US) and no PII is required to integrate with WileyPLUS. The only PII Wiley would accept is user first and last name.	**Yes**	WileyPLUS is fully compliant with FERPA (US) and no PII is required to integrate with WileyPLUS. The only PII Wiley would accept is user first and last name.
SL.154	SL.154 Do agreements with third parties who have access or potential access to Scoped Data, address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of Scoped Data?	**No**		**Yes**	
SL.155	SL.155 Is a business associate contract in place to address obligations for the privacy and security requirements for the services provided?	**Yes**		**Yes**	
SL.156	SL.156 For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, list the countries.	**Yes**	Wiley may transfer your personal information outside of your country of residence for the following reasons: In order to process your transactions. This may occur on servers in countries other than the country where you live. Wiley has servers and major office locations in several countries, in particular in the United States, the United Kingdom, Germany, Singapore, Brazil, India and Australia and has service providers located in India and the Philippines amongst other countries. Such processing may include, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. In order to satisfy global reporting requirements. Wiley may be required to provide your personal information to Wiley affiliates in other countries. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy and all applicable data protection laws.	**No**	

SL.157	SL.157 Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.	**No**	Wiley will not disclose your personal information to any third party except as follows: Where necessary in connection with services provided by intermediaries, who are required to comply with this policy. These service providers provide us with a wide range of office, administrative, information technology, production and business management services; · If you voluntarily provide information in response to an advertisement, with the third party serving the advertisement;		
SL.158	SL.158 Are there contractual controls to ensure that personal information transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure? If yes, describe. If no, explain reason.				
SL.159	SL.159 Is personal information accessed, disclosed, processed, transmitted or retained with third parties outside the US? If yes, describe and list the countries.			**No**	
SL.160	SL.160 Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of the client?			**Yes**	
SL.161	SL.161 Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.	**No**		**No**	
SL.162	SL.162 Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	**Yes**		**Yes**	
SL.163	SL.163 Prohibition of disabling anti-malware with exceptions requiring Security approval and reenablement as soon as possible.	**Yes**		**Yes**	
SL.164	SL.164 Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituents and an owner assigned to maintain and review the policy?	**Yes**		**Yes**	
SL.165	SL.165 Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?	**No**	Vulnerability scans are performed throughout the application life-cycle and scanned as part of the Vulnerability Management Program.	**No**	
SL.166	SL.166 Are vulnerability scans performed against internal networks and systems?	**Yes**		**Yes**	
SL.167	SL.167 Are penetration tests performed?	**Yes**		**Yes**	

SL.168	SL.168 Are there processes to manage threat and vulnerability assessment tools and the data they collect?	**Yes**		**Yes**	
SL.169	SL.169 Are Servers used for transmitting, processing or storing Scoped Data?	**Yes**		**Yes**	
SL.170	SL.170 Are systems and applications patched?	**Yes**		**Yes**	
SL.171	SL.171 Are default hardened base virtual images applied to virtualized operating systems?	**No**		**No**	
SL.172	SL.172 Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?	**Yes**		**Yes**	