CAIQ v3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

| Control Group | CSSD | CID | Control Specification | Consensus Assessment Questions | Consensus Assessment Answers: Yes | No | Not Applicable | Notes | ICOFA TSC 2004 | ICOFA Trust Service Criteria (SOC 2SM Report) | ICOFA TSC 2014 | BITS Shared Assessments AUP v5.0 | BITS Shared Assessments SIG v6.0 | BSI Germany | Canada PIPEDA | CCM V1.4 | CobIT 4.1 | COBIT 5.0 | COPPA | CSA Enterprise Architecture (Formerly the Trusted Cloud Initiative) Domain / Content / Capability | Public | Private | CSA Guidance V3.0 | ENISA IAF | NIST800-53 Rev4 | PCI DSS v3.0 Requirements and Security Assessment Procedures | PCI DSS v3.0 Requirements and Security Assessment Procedures | PCI DSS v3.0 Requirements and Security Assessment Procedures

| | | |

| | | |

| | | |

| | | |

		SP-TM-2		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	X			La macchina virtuale provvede dei requisiti minimi descritti nel documento denominato "Tenyfacilities - Procedura di riversibilità del Servizio SaaS". L'erogazione dei moduli attivati dal cliente, e dalla stima sul numero di utenti utilizzatori del servizio SaaS del cliente, determinazione la macchina virtuale al fine di verificare un alto tasso di performance.	Acquisire dalla sezione sistemi assessing and related security policies.																															
		SP-TM-3		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	X																																									
Infrastructure & Virtualization Security Management - Vulnerability Management	IVS-01	IVS-01	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?			X	Non esiste il layer di virtualizzazione, se ne occupa il nostro fornitore Amazon AWS.																																							
Infrastructure & Virtualization Security - Network Security	IVS-02	IVS-02	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	Do your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X		IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	C.2 A.1 A.2 A.14 A.17 A.18 1.3	CC6.1, CC6.6, CC6.7, CC6.8, CC7.1, CC7.2, CC7.3, CC7.4, A.1.1, A.1.2, A.1.3, A.1.4, A.1.5, A.1.6, A.1.7, A.1.8		Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-09																																
				Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X																																								
				Does you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X																																								
				Are all firewall access control lists documented with business justification?	X			Documentazione degli amministratori delle macchine linux																																				
Infrastructure & Virtualization Security - Hardening and Base Controls	IVS-03	IVS-03	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?			X	Linux aperte solamente le porte necessarie all'utilizzo del servizio.																																							
Infrastructure & Virtualization Security - Production/ Non-Production Environments	IVS-04	IVS-04	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Requests for access across environments may include stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	Do your IaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?			X		IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	B.1	C.2.7.1, C.2.20, C.2.37, C.2.22.2, C.2.10.1, C.2.22.10-14, A.1.1	CF-09	Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-06	CSMT-5 1.255.7																																
				Do your IaaS or PaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X																																								
				Do you logically and physically segregate production and non-production environments?	X																																								
Infrastructure & Virtualization Security - Segmentation	IVS-05	IVS-05	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations.	Are systems and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X				IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	C.17	C.2.7, C.2.9.1, C.2.13		Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-09	CSMT-5 1.255.10																																
				Are systems and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	X																																								
				Are systems and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	X																																								
				Are systems and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X																																								
Infrastructure & Virtualization Security - VM Security - vMotion Data Protection	IVS-06	IVS-06	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?			X																																						
				Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?			X																																						
Infrastructure & Virtualization Security - Hypervisor Hardening	IVS-07	IVS-07	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS-encapsulated communications to the administration consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?			X																																								
Infrastructure & Virtualization Security - Hypervisor Security - Restriction of Administrative Access	IVS-08	IVS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Dalle reti wifi aziendale non è possibile accedere alle macchine virtuali che ospitano il servizio SaaS	IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	C.1 A.1 A.2 A.4 A.15 A.17 A.18	A.1.1, C.2.2.6, C.2.3, C.2.2.6, C.2.2.7, C.2.2.8, C.2.2.9, C.2.2.10, C.2.2.11, C.2.2.12, C.2.2.13, C.2.2.14, C.2.2.15, C.2.2.16, C.2.2.17, C.2.2.18, C.2.2.19, C.2.2.20, C.2.2.21, C.2.2.22, C.2.2.23, C.2.2.24, C.2.2.25, C.2.2.26, C.2.2.27, C.2.2.28, C.2.2.29, C.2.2.30, C.2.2.31, C.2.2.32, C.2.2.33, C.2.2.34, C.2.2.35, C.2.2.36, C.2.2.37, C.2.2.38, C.2.2.39, C.2.2.40, C.2.2.41, C.2.2.42, C.2.2.43, C.2.2.44, C.2.2.45, C.2.2.46, C.2.2.47, C.2.2.48, C.2.2.49, C.2.2.50, C.2.2.51, C.2.2.52, C.2.2.53, C.2.2.54, C.2.2.55, C.2.2.56, C.2.2.57, C.2.2.58, C.2.2.59, C.2.2.60, C.2.2.61, C.2.2.62, C.2.2.63, C.2.2.64, C.2.2.65, C.2.2.66, C.2.2.67, C.2.2.68, C.2.2.69, C.2.2.70, C.2.2.71, C.2.2.72, C.2.2.73, C.2.2.74, C.2.2.75, C.2.2.76, C.2.2.77, C.2.2.78, C.2.2.79, C.2.2.80, C.2.2.81, C.2.2.82, C.2.2.83, C.2.2.84, C.2.2.85, C.2.2.86, C.2.2.87, C.2.2.88, C.2.2.89, C.2.2.90, C.2.2.91, C.2.2.92, C.2.2.93, C.2.2.94, C.2.2.95, C.2.2.96, C.2.2.97, C.2.2.98, C.2.2.99, C.2.2.100, C.2.2.101, C.2.2.102, C.2.2.103, C.2.2.104, C.2.2.105, C.2.2.106, C.2.2.107, C.2.2.108, C.2.2.109, C.2.2.110, C.2.2.111, C.2.2.112, C.2.2.113, C.2.2.114, C.2.2.115, C.2.2.116, C.2.2.117, C.2.2.118, C.2.2.119, C.2.2.120, C.2.2.121, C.2.2.122, C.2.2.123, C.2.2.124, C.2.2.125, C.2.2.126, C.2.2.127, C.2.2.128, C.2.2.129, C.2.2.130, C.2.2.131, C.2.2.132, C.2.2.133, C.2.2.134, C.2.2.135, C.2.2.136, C.2.2.137, C.2.2.138, C.2.2.139, C.2.2.140, C.2.2.141, C.2.2.142, C.2.2.143, C.2.2.144, C.2.2.145, C.2.2.146, C.2.2.147, C.2.2.148, C.2.2.149, C.2.2.150, C.2.2.151, C.2.2.152, C.2.2.153, C.2.2.154, C.2.2.155, C.2.2.156, C.2.2.157, C.2.2.158, C.2.2.159, C.2.2.160, C.2.2.161, C.2.2.162, C.2.2.163, C.2.2.164, C.2.2.165, C.2.2.166, C.2.2.167, C.2.2.168, C.2.2.169, C.2.2.170, C.2.2.171, C.2.2.172, C.2.2.173, C.2.2.174, C.2.2.175, C.2.2.176, C.2.2.177, C.2.2.178, C.2.2.179, C.2.2.180, C.2.2.181, C.2.2.182, C.2.2.183, C.2.2.184, C.2.2.185, C.2.2.186, C.2.2.187, C.2.2.188, C.2.2.189, C.2.2.190, C.2.2.191, C.2.2.192, C.2.2.193, C.2.2.194, C.2.2.195, C.2.2.196, C.2.2.197, C.2.2.198, C.2.2.199, C.2.2.200, C.2.2.201, C.2.2.202, C.2.2.203, C.2.2.204, C.2.2.205, C.2.2.206, C.2.2.207, C.2.2.208, C.2.2.209, C.2.2.210, C.2.2.211, C.2.2.212, C.2.2.213, C.2.2.214, C.2.2.215, C.2.2.216, C.2.2.217, C.2.2.218, C.2.2.219, C.2.2.220, C.2.2.221, C.2.2.222, C.2.2.223, C.2.2.224, C.2.2.225, C.2.2.226, C.2.2.227, C.2.2.228, C.2.2.229, C.2.2.230, C.2.2.231, C.2.2.232, C.2.2.233, C.2.2.234, C.2.2.235, C.2.2.236, C.2.2.237, C.2.2.238, C.2.2.239, C.2.2.240, C.2.2.241, C.2.2.242, C.2.2.243, C.2.2.244, C.2.2.245, C.2.2.246, C.2.2.247, C.2.2.248, C.2.2.249, C.2.2.250, C.2.2.251, C.2.2.252, C.2.2.253, C.2.2.254, C.2.2.255, C.2.2.256, C.2.2.257, C.2.2.258, C.2.2.259, C.2.2.260, C.2.2.261, C.2.2.262, C.2.2.263, C.2.2.264, C.2.2.265, C.2.2.266, C.2.2.267, C.2.2.268, C.2.2.269, C.2.2.270, C.2.2.271, C.2.2.272, C.2.2.273, C.2.2.274, C.2.2.275, C.2.2.276, C.2.2.277, C.2.2.278, C.2.2.279, C.2.2.280, C.2.2.281, C.2.2.282, C.2.2.283, C.2.2.284, C.2.2.285, C.2.2.286, C.2.2.287, C.2.2.288, C.2.2.289, C.2.2.290, C.2.2.291, C.2.2.292, C.2.2.293, C.2.2.294, C.2.2.295, C.2.2.296, C.2.2.297, C.2.2.298, C.2.2.299, C.2.2.300, C.2.2.301, C.2.2.302, C.2.2.303, C.2.2.304, C.2.2.305, C.2.2.306, C.2.2.307, C.2.2.308, C.2.2.309, C.2.2.310, C.2.2.311, C.2.2.312, C.2.2.313, C.2.2.314, C.2.2.315, C.2.2.316, C.2.2.317, C.2.2.318, C.2.2.319, C.2.2.320, C.2.2.321, C.2.2.322, C.2.2.323, C.2.2.324, C.2.2.325, C.2.2.326, C.2.2.327, C.2.2.328, C.2.2.329, C.2.2.330, C.2.2.331, C.2.2.332, C.2.2.333, C.2.2.334, C.2.2.335, C.2.2.336, C.2.2.337, C.2.2.338, C.2.2.339, C.2.2.340, C.2.2.341, C.2.2.342, C.2.2.343, C.2.2.344, C.2.2.345, C.2.2.346, C.2.2.347, C.2.2.348, C.2.2.349, C.2.2.350, C.2.2.351, C.2.2.352, C.2.2.353, C.2.2.354, C.2.2.355, C.2.2.356, C.2.2.357, C.2.2.358, C.2.2.359, C.2.2.360, C.2.2.361, C.2.2.362, C.2.2.363, C.2.2.364, C.2.2.365, C.2.2.366, C.2.2.367, C.2.2.368, C.2.2.369, C.2.2.370, C.2.2.371, C.2.2.372, C.2.2.373, C.2.2.374, C.2.2.375, C.2.2.376, C.2.2.377, C.2.2.378, C.2.2.379, C.2.2.380, C.2.2.381, C.2.2.382, C.2.2.383, C.2.2.384, C.2.2.385, C.2.2.386, C.2.2.387, C.2.2.388, C.2.2.389, C.2.2.390, C.2.2.391, C.2.2.392, C.2.2.393, C.2.2.394, C.2.2.395, C.2.2.396, C.2.2.397, C.2.2.398, C.2.2.399, C.2.2.400	10.2 10.2.1	Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-10	CSMT-5 1.255.5 CSMT-5 1.255.7 CSMT-5 1.255.8 CSMT-5 1.255.10	DP-09 DP-10 DP-11 DP-12 DP-13 DP-14 DP-15 DP-16 DP-17 DP-18 DP-19 DP-20 DP-21 DP-22 DP-23 DP-24 DP-25 DP-26 DP-27 DP-28 DP-29 DP-30 DP-31 DP-32 DP-33 DP-34 DP-35 DP-36 DP-37 DP-38 DP-39 DP-40 DP-41 DP-42 DP-43 DP-44 DP-45 DP-46 DP-47 DP-48 DP-49 DP-50 DP-51 DP-52 DP-53 DP-54 DP-55 DP-56 DP-57 DP-58 DP-59 DP-60 DP-61 DP-62 DP-63 DP-64 DP-65 DP-66 DP-67 DP-68 DP-69 DP-70 DP-71 DP-72 DP-73 DP-74 DP-75 DP-76 DP-77 DP-78 DP-79 DP-80 DP-81 DP-82 DP-83 DP-84 DP-85 DP-86 DP-87 DP-88 DP-89 DP-90 DP-91 DP-92 DP-93 DP-94 DP-95 DP-96 DP-97 DP-98 DP-99 DP-100 DP-101 DP-102 DP-103 DP-104 DP-105 DP-106 DP-107 DP-108 DP-109 DP-110 DP-111 DP-112 DP-113 DP-114 DP-115 DP-116 DP-117 DP-118 DP-119 DP-120 DP-121 DP-122 DP-123 DP-124 DP-125 DP-126 DP-127 DP-128 DP-129 DP-130 DP-131 DP-132 DP-133 DP-134 DP-135 DP-136 DP-137 DP-138 DP-139 DP-140 DP-141 DP-142 DP-143 DP-144 DP-145 DP-146 DP-147 DP-148 DP-149 DP-150 DP-151 DP-152 DP-153 DP-154 DP-155 DP-156 DP-157 DP-158 DP-159 DP-160 DP-161 DP-162 DP-163 DP-164 DP-165 DP-166 DP-167 DP-168 DP-169 DP-170 DP-171 DP-172 DP-173 DP-174 DP-175 DP-176 DP-177 DP-178 DP-179 DP-180 DP-181 DP-182 DP-183 DP-184 DP-185 DP-186 DP-187 DP-188 DP-189 DP-190 DP-191 DP-192 DP-193 DP-194 DP-195 DP-196 DP-197 DP-198 DP-199 DP-200 DP-201 DP-202 DP-203 DP-204 DP-205 DP-206 DP-207 DP-208 DP-209 DP-210 DP-211 DP-212 DP-213 DP-214 DP-215 DP-216 DP-217 DP-218 DP-219 DP-220 DP-221 DP-222 DP-223 DP-224 DP-225 DP-226 DP-227 DP-228 DP-229 DP-230 DP-231 DP-232 DP-233 DP-234 DP-235 DP-236 DP-237 DP-238 DP-239 DP-240 DP-241 DP-242 DP-243 DP-244 DP-245 DP-246 DP-247 DP-248 DP-249 DP-250 DP-251 DP-252 DP-253 DP-254 DP-255 DP-256 DP-257 DP-258 DP-259 DP-260 DP-261 DP-262 DP-263 DP-264 DP-265 DP-266 DP-267 DP-268 DP-269 DP-270 DP-271 DP-272 DP-273 DP-274 DP-275 DP-276 DP-277 DP-278 DP-279 DP-280 DP-281 DP-282 DP-283 DP-284 DP-285 DP-286 DP-287 DP-288 DP-289 DP-290 DP-291 DP-292 DP-293 DP-294 DP-295 DP-296 DP-297 DP-298 DP-299 DP-300 DP-301 DP-302 DP-303 DP-304 DP-305 DP-306 DP-307 DP-308 DP-309 DP-310 DP-311 DP-312 DP-313 DP-314 DP-315 DP-316 DP-317 DP-318 DP-319 DP-320 DP-321 DP-322 DP-323 DP-324 DP-325 DP-326 DP-327 DP-328 DP-329 DP-330 DP-331 DP-332 DP-333 DP-334 DP-335 DP-336 DP-337 DP-338 DP-339 DP-340 DP-341 DP-342 DP-343 DP-344 DP-345 DP-346 DP-347 DP-348 DP-349 DP-350 DP-351 DP-352 DP-353 DP-354 DP-355 DP-356 DP-357 DP-358 DP-359 DP-360 DP-361 DP-362 DP-363 DP-364 DP-365 DP-366 DP-367 DP-368 DP-369 DP-370 DP-371 DP-372 DP-373 DP-374 DP-375 DP-376 DP-377 DP-378 DP-379 DP-380 DP-381 DP-382 DP-383 DP-384 DP-385 DP-386 DP-387 DP-388 DP-389 DP-390 DP-391 DP-392 DP-393 DP-394 DP-395 DP-396 DP-397 DP-398 DP-399 DP-400	01.B 02.B 03.B 04.B 05.B 06.B 07.B 08.B 09.B 10.B 11.B 12.B 13.B 14.B 15.B 16.B 17.B 18.B 19.B 20.B 21.B 22.B 23.B 24.B 25.B 26.B 27.B 28.B 29.B 30.B 31.B 32.B 33.B 34.B 35.B 36.B 37.B 38.B 39.B 40.B 41.B 42.B 43.B 44.B 45.B 46.B 47.B 48.B 49.B 50.B 51.B 52.B 53.B 54.B 55.B 56.B 57.B 58.B 59.B 60.B 61.B 62.B 63.B 64.B 65.B 66.B 67.B 68.B 69.B 70.B 71.B 72.B 73.B 74.B 75.B 76.B 77.B 78.B 79.B 80.B 81.B 82.B 83.B 84.B 85.B 86.B 87.B 88.B 89.B 90.B 91.B 92.B 93.B 94.B 95.B 96.B 97.B 98.B 99.B 100.B 101.B 102.B 103.B 104.B 105.B 106.B 107.B 108.B 109.B 110.B 111.B 112.B 113.B 114.B 115.B 116.B 117.B 118.B 119.B 120.B 121.B 122.B 123.B 124.B 125.B 126.B 127.B 128.B 129.B 130.B 131.B 132.B 133.B 134.B 135.B 136.B 137.B 138.B 139.B 140.B 141.B 142.B 143.B 144.B 145.B 146.B 147.B 148.B 149.B 150.B 151.B 152.B 153.B 154.B 155.B 156.B 157.B 158.B 159.B 160.B 161.B 162.B 163.B 164.B 165.B 166.B 167.B 168.B 169.B 170.B 171.B 172.B 173.B 174.B 175.B 176.B 177.B 178.B 179.B 180.B 181.B 182.B 183.B 184.B 185.B 186.B 187.B 188.B 189.B 190.B 191.B 192.B 193.B 194.B 195.B 196.B 197.B 198.B 199.B 200.B 201.B 202.B 203.B 204.B 205.B 206.B 207.B 208.B 209.B 210.B 211.B 212.B 213.B 214.B 215.B 216.B 217.B 218.B 219.B 220.B 221.B 222.B 223.B 224.B 225.B 226.B 227.B 228.B 229.B 230.B 231.B 232.B 233.B 234.B 235.B 236.B 237.B 238.B 239.B 240.B 241.B 242.B 243.B 244.B 245.B 246.B 247.B 248.B 249.B 250.B 251.B 252.B 253.B 254.B 255.B 256.B 257.B 258.B 259.B 260.B 261.B 262.B 263.B 264.B 265.B 266.B 267.B 268.B 269.B 270.B 271.B 272.B 273.B 274.B 275.B 276.B 277.B 278.B 279.B 280.B 281.B 282.B 283.B 284.B 285.B 286.B 287.B 288.B 289.B 290.B 291.B 292.B 293.B 294.B 295.B 296.B 297.B 298.B 299.B 300.B 301.B 302.B 303.B 304.B 305.B 306.B 307.B 308.B 309.B 310.B 311.B 312.B 313.B 314.B 315.B 316.B 317.B 318.B 319.B 320.B 321.B 322.B 323.B 324.B 325.B 326.B 327.B 328.B 329.B 330.B 331.B 332.B 333.B 334.B 335.B 336.B 337.B 338.B 339.B 340.B 341.B 342.B 343.B 344.B 345.B 346.B 347.B 348.B 349.B 350.B 351.B 352.B 353.B 354.B 355.B 356.B 357.B 358.B 359.B 360.B 361.B 362.B 363.B 364.B 365.B 366.B 367.B 368.B 369.B 370.B 371.B 372.B 373.B 374.B 375.B 376.B 377.B 378.B 379.B 380.B 381.B 382.B 383.B 384.B 385.B 386.B 387.B 388.B 389.B 390.B 391.B 392.B 393.B 394.B 395.B 396.B 397.B 398.B 399.B 400.B	1.1 1.2 1.3 1.4 1.5 1.6 1.7 1.8 1.9 1.10 1.11 1.12 1.13 1.14 1.15 1.16 1.17 1.18 1.19 1.20 1.21 1.22 1.23 1.24 1.25 1.26 1.27 1.28 1.29 1.30 1.31 1.32 1.33 1.34 1.35 1.36 1.37 1.38 1.39 1.40 1.41 1.42 1.43 1.44 1.45 1.46 1.47 1.48 1.49 1.50 1.51 1.52 1.53 1.54 1.55 1.56 1.57 1.58 1.59 1.60 1.61 1.62 1.63 1.64 1.65 1.66 1.67 1.68 1.69 1.70 1.71 1.72 1.73 1.74 1.75 1.76 1.77 1.78 1.79 1.80 1.81 1.82 1.83 1.84 1.85 1.86 1.87 1.88 1.89 1.90 1.91 1.92 1.93 1.94 1.95 1.96 1.97 1.98 1.99 1.100 1.101 1.102 1.103 1.104 1.105 1.106 1.107 1.108 1.109 1.110 1.111 1.112 1.113 1.114 1.115 1.116 1.117 1.118 1.119 1.120 1.121 1.122 1.123 1.124 1.125 1.126 1.127 1.128 1.129 1.130 1.131 1.132 1.133 1.134 1.135 1.136 1.137 1.138 1.139 1.140 1.141 1.142 1.143 1.144 1.145 1.146 1.147 1.148 1.149 1.150 1.151 1.152 1.153 1.154 1.155 1.156 1.157 1.158 1.159 1.160 1.161 1.162 1.163 1.164 1.165 1.166 1.167 1.168 1.169 1.170 1.171 1.172 1.173 1.174 1.175 1.176 1.177 1.178 1.179 1.180 1.181 1.182 1.183 1.184 1.185 1.186 1.187 1.188 1.189 1.190 1.191 1.192 1.193 1.194 1.195 1.196 1.197 1.198 1.199 1.200 1.201 1.202 1.203 1.204 1.205 1.206 1.207 1.208 1.209 1.210 1.211 1.212 1.213 1.214 1.215 1.216 1.217 1.218 1.219 1.220 1.221 1.222 1.223 1.224 1.225 1.226 1.227 1.228 1.229 1.230 1.231 1.232 1.233 1.234 1.235 1.236 1.237 1.238 1.239 1.240	Annex A.1.1.8 A.12.1.1 A.12.1.2 A.12.1.3 A.12.6.1																																												
Infrastructure & Virtualization Security - Virtual Machine Security - Migration to Production	IVS-09	IVS-09	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	Do your IaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?			X		IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	B.1	C.2.7.1, C.2.20, C.2.37, C.2.22.2, C.2.10.1, C.2.22.10-14, A.1.1	CF-09	Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-06	CSMT-5 1.255.7																																
				Do your IaaS or PaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X																																								
				Do you logically and physically segregate production and non-production environments?	X																																								
Infrastructure & Virtualization Security - Image Security	IVS-10	IVS-10	A system and network environment protection should be deployed when moving a virtual machine from a trusted or hardened image to an untrusted or less hardened image. Vendor supplied baselines should be used when performing such deployments, and configuration baselines should be maintained for each operating system and hypervisor. This should be supported by a documented justification for all allowed services, protocols, and ports, and compensating controls.	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?			X																																								
Infrastructure & Virtualization Security - Information System Regulatory Mapping	IVS-11	IVS-11	Restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?				X																																								
Infrastructure & Virtualization Security - Interoperability & Portability - Virtualization	IVS-12	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)			X	Dalle reti wifi aziendale non è possibile accedere alle macchine virtuali che ospitano il servizio SaaS																																										
				Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	Dalle reti wifi aziendale non è possibile accedere alle macchine virtuali che ospitano il servizio SaaS																																							
Infrastructure & Virtualization Security - Network Architecture	IVS-13	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical controls shall be implemented and supported by a defence-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X		IS-6	ISO-20 Procedures exist to protect against unauthorized access to system resources.	CC6.6	C.1 A.1 A.2 A.4 A.15 A.17 A.18 1.3	A.8.7, A.9.7, A.10, B.9.11, B.10.1, B.10.5, B.9.2, B.9.3, B.9.10		Schedule 1 (Section 5), 6.7 - Safeguards, Subsec. 4.7.3	DA-08																																						
				Do you implement technical measures and apply defence-in-depth techniques (e.g. deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?																																											
Interoperability & Portability - APIs	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			La documentazione sulle API standard presente dal servizio SaaS viene fornita su richiesta specifica del Cliente.																																					
Interoperability & Portability - Data Request	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., doc, xls, pdf, logs, and flat files)	Is unstructured customer data available on request in an industry-standard format (e.g., doc, xls, or pdf)?																																										
Interoperability & Portability - Policy & Legal	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to support interoperability between or among service and cloud providers, including (when applicable) interoperability, and portability for application development and information exchange, usage and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X																																										
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			Le procedure sono descritte nel documento denominato "Tenyfacilities - Procedura di riversibilità del Servizio SaaS"																																							
Interoperability & Portability - Standard/Network Protocols	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are followed.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			La connessione al servizio SaaS è sempre fornita tramite protocollo sicuro "https"																																							
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X																																								
Interoperability & Portability - Virtualization	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			Viene utilizzato il sistema di virtualizzazione VMWare																																							
		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X																																							

Mobile Security *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			Si per Laptop aziendali assegnati ai dipendenti dell'azienda											HR001.03 HR001.06 HR001.07 HR001.08 HR009.03 HR103.04		IRM > Governance Risk & Compliance > Technical Security Awareness and Training	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)												
Mobile Security *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			Nel documento interno denominato "EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale" è presente l'elenco delle applicazioni cloud utilizzate per l'archiviazione dei dati aziendali.											HR001.03 HR001.08 HR009.02 HR103.01 HR103.02 HR103.03		IRM > Policies and Standards > Technical Security Standards	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											6.1.1
Mobile Security *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?		X		Per consentire lo sviluppo e il test dell'applicazione mobile collegata al service SaaS, è necessario consentire l'installazione di applicazioni non provenienti dagli store ufficiali.											HR001.03 HR001.08 HR103.01 HR103.02 HR103.03		ITOS > Service Support > Configuration Management – Software Management	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	Come specificato nel documento interno denominato "EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale", l'utilizzo di dispositivi personali non è autorizzato a scopi lavorativi.											HR001.03 HR001.08 HR103.01 HR103.02 HR103.03		IRM > Policies and Standards > Technical Security Standards	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											
Mobile Security *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			Inoltre il documento interno denominato "EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale"											HR001.03 HR001.08 HR103.01 HR103.02 HR103.03		IRM > Policies and Standards > Technical Security Standards	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											7.3
Mobile Security *Cloud-Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	X			Nel documento interno denominato "EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale" è presente l'elenco delle applicazioni cloud utilizzate per l'archiviazione dei dati aziendali.											HR001.03 HR001.08 HR103.01 HR103.02 HR103.03		IRM > Governance Risk & Compliance > Vendor Management	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											
Mobile Security *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process for test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	X			Gli audit interni prevedono i test delle funzionalità dei servizi SaaS anche su dispositivi mobile in quanti test vengono utilizzati solamente i dispositivi mobile aziendali (IOS e Android).											HR001.03 HR001.08 HR103.01 HR103.02 HR103.03 IM003.07 IM003.08		ITOS > Service Support > Configuration Management – Software Management	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											
Mobile Security *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X	Come specificato nel documento interno denominato "EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale", l'utilizzo di dispositivi personali non è autorizzato a scopi lavorativi.											HR001.03 HR001.08 HR103.01 HR103.02 IM003.01 IM003.06		IRM > Policies and Standards > Information Security Policies	possible	X	None (Mobile Guidance)									Clause 6.1.1, 6.1.1(e)(1) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(2) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3)											

Mobile Security *Device Inventory*	MDS-01	MDS-01	An inventory of all mobile devices used to store and access company data which includes device status (e.g. operating system and patch levels, lost or decommissioned, device assigned)	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g. operating system and patch levels, lost or decommissioned, device assigned)?	X																	MDM>Mobile Endpoint Protection Services>End Point-Inventory Control	possible	X	None (Mobile Guidance)									Clause 4.3.1 4.3.2 4.3.3(a)(1) 4.3.2 4.3.2(a)(1) 4.3.2(d)(f), 4.3.2(b) 4.3.2 (c) 4.3.2(c)(1), 4.3.2(c)(2) 4.3.2(d) 4.3.2(d)(1) 4.3.2(d)(2) 4.3.2(d)(3) 4.3.2(e) 4.3.2(e)(1) 4.3.2(e)(2) 4.3.2(f) 4.3.2(g) 4.3.3(b) 4.3 4.4 4.4(a), 4.4(b) 4.4(c) 4.4(d) 4.4(e) 4.4(f) 4.4(g) 4.4(h) 4.4(i) 4.4(j) 4.4(k) 4.4(l) 4.4(m) 4.4(n) 4.4(o) 4.4(p) 4.4(q) 4.4(r) 4.4(s) 4.4(t) 4.4(u)														
Mobile Security *Device Management*	MDS-02	MDS-02	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																										
Mobile Security *Encryption*	MDS-03	MDS-03	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?		X																																								
Mobile Security *Jailbreaking and Rooting*	MDS-04	MDS-04	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and enforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting)?		X		Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																										
		MDS-04.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?				Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																									
Mobile Security *Legal*	MDS-05	MDS-05.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	X																																									
		MDS-05.2		Do you have detective and preventive controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?				Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																									
Mobile Security *Lockout Screen*	MDS-06	MDS-06	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company-owned devices?	X																																								
Mobile Security *Operating Systems*	MDS-07	MDS-07.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																									
Mobile Security *Passwords*	MDS-08	MDS-08.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise-issued mobile devices and/or BYOD mobile devices?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																									
		MDS-08.2		Are your password policies enforced through technical controls (i.e. MDM)?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi.																																									
		MDS-08.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X																																								
Mobile Security *Policy*	MDS-17	MDS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	X																																								
		MDS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	X																																								
		MDS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	X																																								
Mobile Security *Remote Wipe*	MDS-18	MDS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	X			Lesse specificato nel documento interoperamento-Responsabilità – Piano di consapevolezza dei dipendenti sulla sicurezza aziendale", è vietato ai dipendenti dell'azienda di trasferire i dati aziendali sui dispositivi personali.																																									
		MDS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			Ogni laptop aziendale assegnato ai dipendenti dell'azienda																																						
Mobile Security *Security Patches*	MDS-19	MDS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi. I dispositivi (pc, laptop) sono costantemente aggiornati sulle ultime patch di sicurezza.																																									
		MDS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	X			Tutti i dispositivi (pc, laptop) sono gestiti centralmente dal reparto IT di Zucchetti, che governa ed eventualmente interviene, a richiesta del responsabile di Easytelleff, l'operatività sui specifici dispositivi. I dispositivi (pc, laptop) sono costantemente aggiornati sulle ultime patch di sicurezza.																																									
Mobile Security *Users*	MDS-20	MDS-20.1	The BYOD policy shall clarify the systems and services allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?		X		L'accesso ai server che esplorano le macchine virtuali contenenti il servizio SaaS è limitato agli IP dei dispositivi aziendali autorizzati.																																									
		MDS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?		X		L'accesso ai server che esplorano le macchine virtuali contenenti il servizio SaaS è limitato agli IP dei dispositivi aziendali autorizzati.																																									
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a business investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X										CC9.3																																				12.5.3 12.10.1
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			Utilizziamo del sistema informatico di ticketing vengono archiviati tutti i malfunzionamenti, e l'analisi triennale, dei service fault	9.1.7.7	9.1	7.1, 7.1.2	16 (B) 16 (1) 16 (2) 16 (3) 16 (4) 16 (5)	Schedule 1 (Section 6) 6.1 Accountability, Subs. 6.1.2, 6.1.3(perform), Subs. 6.8.2	9-22	CSBP-6.1-DIS-8	MPDS-DS-DIS-01 MPDS-DS-DIS-02 MPDS-DS-DIS-03 MPDS-DS-DIS-04 MPDS-DS-DIS-05 MPDS-DS-DIS-06 MPDS-DS-DIS-07 MPDS-DS-DIS-08 MPDS-DS-DIS-09 MPDS-DS-DIS-10 MPDS-DS-DIS-11	9.1.8 and 10.2.10	DS06 > Compliance Contact/Authority Maintenance	Shared	X																																							
									10.1.1	10.1		16.1(1) Procedures exist to identify, report, and act upon system security breaches and other incidents.																																								
												16.1(2) Procedures exist to provide that issues of noncompliance with system availability, confidentiality of data, processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.																																									
				Do you provide customized breach requirements into your security incident response plans?	X																																									
				Do you provide roles and responsibilities document specifying which you or your tenants are responsible for during security incidents?	X			Disponiamo di un documento in cui vengono specificate le responsabilità dell'azienda nei confronti dei vostri clienti ai fini/eventi di un malfunzionamento (livelli di severità), quelle informazioni sono anche presenti nel contratto di fornitura ai vostri clienti.	10.3(2)																																									
				Have you tested your security incident response plans in the last year?	X																																									
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	X				12.2.2 12.5.2 12.5.3	9.2 9.3	7.1, 7.1.4	16 (B) 16 (H) 16 (M) 16 (N)	Schedule 1 (Section 6) 6.1 Accountability, Subs. 6.1.3	9-23	CSBP-6.1-DIS-8	MPDS-DS-DIS-01 MPDS-DS-DIS-06 MPDS-DS-DIS-07 MPDS-DS-DIS-08 MPDS-DS-DIS-09 MPDS-DS-DIS-10 MPDS-DS-DIS-11	9.1.5, 9.1.8 and 9.2.10	DS06 > Human Resources Security > Employee Awareness	Shared	X																																							
				Do you log and monitor security incident information, metrics and other data in a manner supporting their use in future legal proceedings?	X				12.5.3	9.3	7.1, 7.1.1, 7.1.2, 7.4		Schedule 1 (Section 6) 6.1 Accountability, Subs. 6.1.3	9-24	CSBP-6.1-DIS-8	MPDS-DS-DIS-01 MPDS-DS-DIS-06 MPDS-DS-DIS-07 MPDS-DS-DIS-08 MPDS-DS-DIS-09 MPDS-DS-DIS-10 MPDS-DS-DIS-11	9.1.8 and 9.2.10	DS06 > Legal Services > Incident Response Legal	Shared	X																																							
				Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X				12.5.3 12.5.4	9.3																																					

Security Incident Response Legal Preparation	SEF-04	SEF-04.1	Incident, Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X																	Preparation																					
		SEF-04.2		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			4A.15.0																																			
		SEF-04.3		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X																																					
Security Incident Management, E-Discovery & Cloud Forensics	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	X			15.0.0	CC9.2 CC9.1		7.2	17.2b)		25-25	CSM7-1.1 DS-2.9				ISO/IEC 27	312.8 and 312.10	ITOS > Operations Risk Management > Key Risk Indicators	Shared	Domain 2	6.07.01. (a) 6.07.01. (j)		NIST SP 800-53 R5 IR-4 NIST SP 800-53 R5 IR-5 NIST SP 800-53 R5 IR-6	2.7 2.10	21 CFR 164.308 (a)(1)(i)(D)	4.19.2.2	4.19.3.8		CP-10IR-5 IR-1	IR-6 IR-5 IR-8		7.2 7.5	PS11	IRMP	ISO/IEC v2.0 12.5.6	
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	X				Su richiesta del Cliente è possibile fornire l'elenco dei malfunzionamenti registrati in un range temporale																																		
Supply Chain Management, Transparency and Accountability Network Governance	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X																	MRA > Governance Risk & Compliance > Vendor Management	Provider	Domain 2																				
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X				Nel caso di colluogo sul servizio Saab di collaborazione oppure azienda esterna, il contratto viene regolamentato dal servizio legale del Saab e di norma non consentito. Si colluogo delle funzionalità da parte del fornitore viene opportunamente testata dal dipendente di Saab/staff di esterna degli audit interni. In caso particolare in cui sia necessario fornire ai fornitori l'accesso a delle macchine virtuali di test (mai su quelle in produzione) gli access alle carte/file è limitato al lavoro da svolgere.																															
Supply Chain Management, Transparency and Accountability Incident Reporting	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	X				Su richiesta del Cliente è possibile fornire l'elenco dei malfunzionamenti registrati in un range temporale									ISO/IEC 27		ITOS > Service Support > Incident Management > Cross Cloud Incident Response	Provider	Domain 2																				
Supply Chain Management, Transparency and Accountability Service Agreements	STA-03	STA-03.1	Business critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and system components, shall be designed, developed, and deployed in accordance with	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			22.2.0	CC 2.2 The systems security, availability, system integrity, and confidentiality and related security obligations of users and the entity's system security, availability, system integrity, and	CC2.2 CC2.3	2.2	2.2.6, 6.9.9	09.0b) 79.0b)	Schedule 1 (Section 31, 6.7 - Safeguards, Subsec. 4.7.3	27001:2013	ISO/IEC 01 ISO/IEC 01 ISO/IEC 02 ISO/IEC 07	312.8 and 312.10	ITOS > Service Delivery > Service Level Management	possible	Domain 2	6.02.(c) 6.03.07. (a) 6.03.07. (b) 6.03.07. (c)	Article 17	NIST SP 800-53 R3 CA-9 NIST SP 800-53 R3 SA-9	6.2.2 6.2.5		4.8.2.3 4.10.6.2	4.15.1.2 4.15.1.2		Commandment #6 Commandment #7 Commandment #8			SC-08 SC-11 SC-22 SC-23	17.1	PA3 TVM PA06	IRMP BRDP SDP	
		STA-03.2		Do you provide tenants with capacity planning and use reports?	X				Su richiesta del cliente.																																		
Supply Chain Management, Transparency and Accountability Provider Internal Assessments	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X															MRA > Governance Risk & Compliance > Vendor Management	possible	Domain 2																				12.1.1
Supply Chain Management, Transparency and Accountability Third-Party Agreements	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually agreed-upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effective governance, risk management, assessment, and assurance of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	X			4A.6.0	CC2.2 CC2.3 CC6.5 CC6.6 CC6.7		2.2	2.2.1, 2.2.4, 6.4.1, 6.4.2, 6.4.3	09.0b) 79.0c) 79.0c) 79.0c) 79.0c) 79.0c) 0.0.7.1. (h)	Schedule 1 (Section 31, 6.1 Accountability, Subs. 4.1.3	ISO-02	CSM7-0.1 DS5.11	ISO/IEC 09 ISO/IEC 05	312.5, 312.8 and 312.10	ITOS > Legal Services > contracts	Shared	Domain 9	6.02. (a) 6.10. (h) 6.10. (i)	Article 17 (3)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4) NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)		2.1.5		4.4.2.3 4.10.2.1 4.10.8.2 4.11.4.6 4.11.3.1 4.12.3.1 4.12.5.6	4.19.5.a 4.07.a partial, 4.19.2.2 4.9.4.1 4.9.11.1	27002:2005 ISO/IEC 27005 STBL 2-5b	3.138.17 SAR 23 CFR 1.2	Commandment #6 Commandment #8 Commandment #9 Commandment #7 Commandment #8	Chapter 9 Article 14,		CA-3 MP-5 PS-7 SA-4 SA-9	5.2 -1.2			PO-DSN v2.0 7.2.4 PO-DSN v2.0 7.2.8.2	7.2 7.2.8.2
		STA-05.2		Does legal counsel review all third-party agreements?	X				Nel caso di colluogo sul servizio Saab di collaborazione oppure azienda esterna, il contratto viene regolamentato dal servizio legale del Saab/ partner saabitaria (Saabelle)																																		
		STA-05.3		Do third-party agreements include provision for the security and protection of information and assets?	X				Nel caso di colluogo sul servizio Saab di collaborazione oppure azienda esterna, il contratto viene regolamentato dal servizio legale del Saab/ partner saabitaria (Saabelle)																																	
		STA-05.4		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	X				Consente su richiesta da parte del Cliente																																	
Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X													ISO/IEC 01 ISO/IEC 05 MRA01			MRA > Governance Risk & Compliance > Vendor Management	possible																			12.8.1
Supply Chain Management, Transparency and Accountability Supply Chain Metrics	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identify non-conformance to established agreements. The review should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X				Se per quanto riguarda l'allineamento degli SLA garantiti dall'azienda degli SLA del fornitore Amazon AWS (per lo continuità di funzionamento del servizio SaaS), non sono invece previste procedure di allineamento degli SLA tra l'azienda e i fornitori di sviluppo software, in quanto gli sviluppi assegnati non sono mai di tipo core.				01.00)			ISO/IEC 01 ISO/IEC 05 ISO/IEC 06 ISO/IEC 05 ISO/IEC 01 ISO/IEC 02 ISO/IEC 06		ITOS > Service Delivery > Service Level Management > Vendor Management	possible	Domain 5	6.02. (c) 6.02. (d) 6.07.01. (b)																				
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X																																						
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X																																						
		STA-07.4		Do you review all agreements, policies and processes at least annually?	X				contratti di fornitura hanno una durata massima annuale.																																	
Supply Chain Management, Transparency and Accountability Third-Party Assessment	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third-party providers upon which their information supply chain depends on	Do you assure reasonable information security across your information supply chain by performing an annual review?	X													ISO/IEC 01 MRA01 MRA02			MRA > Governance Risk & Compliance > Vendor Management	possible	Domain 2																				
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?		X			Da you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?																																		
Supply Chain Management, Transparency and Accountability Third-Party Audits	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain	Do you permit tenants to perform independent vulnerability assessments?	X			15.1.0	CC 1.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	CC2.2 CC2.3 CC4 CC5.5		1.1, 1.2, 1.4, 1.7, 1.9	79.0b) 79.0c) 79.0c) 79.0c) 84.0b)		CO-05	CSM7-1.1 IM7-2.6, IM-2.1, DS 2.4	ISO/IEC 08 ISO/IEC 05 MRA01	312.2(a) and 312.5 (Prohibition on Disclosure)	ITOS > Compliance > Third Party Audits	Shared	Domain 2, 4	6.10. (a) 6.10. (b) 6.10. (d) 6.10. (e) 6.10. (g)		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1	2.2.2 2.2.4 2.2.5 2.2.11 4.2.2	21 CFR 164.308(a)(1) Deal	4.4.2.3 4.10.2.1 4.10.8.2 4.10.8.2	4.19.1.2 4.07.a partial, 4.19.2.2 4.15.1.2		Commandment #1 Commandment #2 Commandment #3	Chapter 9 Article 14, 21		AC-1 AT-1 AU-1 CA-1 CM-1	5.8			PO-DSN v2.0 7.2.4 PO-DSN v2.0 7.2.8.2 PO-DSN v2.0 12.8.2 PO-DSN v2.0 Appendix A	7.2.4 7.2.8.2 12.8.2 Appendix A
Threat and Vulnerability Management Antivirus / Malicious Software	THV-01	THV-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for prevention, detection, and timely response to malicious attacks on all of your systems and network components managed or managed-user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or correct to your cloud service offerings installed on all of your systems?	X			15.5.0	CC5.8			5.7	17.0b)			CSM7-1.1 DS5.9	ISO/IEC 01 ISO/IEC 02 ISO/IEC 02 ISO/IEC 01	312.8 and 312.10	MRA > Infrastructure Protection Services > Anti-Virus	Shared	Domain 2	6.03. (f)	Article 17	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-5 NIST SP 800-53 R3 SI-7	6.2.2	45 CFR 164.308 (a)(5)(ii)(B)	4.10.1.1	4.7.2.1		Commandment #6 Commandment #8			SI-03 SI-05 SI-07 SI-08	14.1 17.8	PA1	IRMP	PO-DSN v2.0 5.1 PO-DSN v2.0 5.1.2 PO-DSN v2.0 5.5.2	5.1.2 5.5
Threat and Vulnerability Management Vulnerability / Patch Management	THV-02	THV-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based ranking of all identified vulnerabilities shall be used.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			15.10.0	SIS.30.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC7.1	4	1.1.5.2, 1.3	02.0b) 79.0b)	Schedule 1 (Section 31, 6.7 - Safeguards, Subsec. 4.7.3	9-20	CSM7-1.1 AM-1.2 CSM7-1.1 IM-3	ISO/IEC 01 ISO/IEC 01 ISO/IEC 02 ISO/IEC 06 ISO/IEC 06 ISO/IEC 05 ISO/IEC 01 ISO/IEC 05 ISO/IEC 01	312.8 and 312.10	MRA > Threat and Vulnerability Management > Vulnerability Management	Shared	Domain 2	6.03.02. (a) 6.03.02. (b) 6.03.05. (c) 6.07.01. (a)	Article 17	NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-8 (2) NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (8) NIST SP 800-53 R3 RA-5 (9) NIST SP 800-53 R3 SC-00 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-6	1.2.6 2.7	45 CFR 164.308 (a)(5)(ii)(B) 45 CFR 164.308 (a)(8) 45 CFR 164.308 (a)(8)(ii)(B)	4.12.3.1 4.12.5.2 4.12.6.1	4.7.a partial, 4.12.5.2 4.12.6.1 4.12.2.1		Commandment #6 Commandment #8			CM-1 CM-6 CM-8 RA-5 RA-6 RA-7 RA-8 RA-9 RA-10 SC-00 SI-1 SI-2 SI-3 SI-6	12.4 16.1	PA2 TVM	IRMP	PO-DSN v2.0 7.2.2 PO-DSN v2.0 8.1 PO-DSN v2.0 8.1.2 PO-DSN v2.0 8.2 PO-DSN v2.0 8.4.5 PO-DSN v2.0 8.5 PO-DSN v2.0 8.6 PO-DSN v2.0 11.2 PO-DSN v2.0 11.2.3	7.2 8.1 8.1.2 8.2 8.4.5 8.5 8.6 11.2 11.2.3
Threat and Vulnerability Management Mobile Code	THV-03	THV-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	X			15.4.0	CC5.8 CC7.1			2.2.0.12, 1.2.5		06-15		ISO/IEC 01 ISO/IEC 02 ISO/IEC 02 ISO/IEC 05 ISO/IEC 01 ISO/IEC 05	312.8 and 312.10	MRA > Infrastructure Protection Services > End Point - Mobile Utility	Shared	Domain 10	6.03. (g)	Article 17	NIST SP 800-53 R3 SI-4			4.10.2.2 4.12.2.2	4.12.2.1		Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11			SI-14				PO-DSN v2.0 8.1 PO-DSN v2.0 8.1.2 PO-DSN v2.0 8.2 PO-DSN v2.0 8.5 PO-DSN v2.0 8.6 PO-DSN v2.0 11.2.1 PO-DSN v2.0 11.2.3	8.1 8.1.2 8.2 8.5 8.6 11.2 11.2.3

© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer,