Chapter	Item	Relevant control (Y/N)	Control item	Link to the evidence + document and page number and/or article number
Risk management	Is there an up to date inventory of assets (infrastructure, applications…)?	Y	System uptime page	https://status.wildix.com
	Is there a formal assessment of the sensitivity of assets with respect to availability, confidentiality & integrity?	Y	Wildix utilizes OWASP practices such as Application Risk Profile and Risk Rating to manage assets and vulnerabilities.	
Data protection	Are devices storing personal data identified?	Y	WMS, as managed by the Wildix Partner, identifies all devices that store personal data	https://wildix.atlassian.net/wiki/x/hhbOAQ, under sub-header "Devices management"
	Are sensitive personal data encrypted?	N	Wildix does not store sensitive personal data (managed by Wildix Partners)	

	Are encryption mechanisms non vulnerable?	**Y**	Wildix systems all automatically implement the following non-vulnerable encryption mechanisms: -TLS encryption of HTTPS traffic to the PBX, screen sharing sessions, Wizyconf conferences -SIP TLS - SIP signalling over TLS -SRTP - SDES-AES 128 encryption of voice / audio, including Wizyconf conferences -DTLS-SRTP - TLS encryption of voice / audio, including Wizyconf conferences -VPN AES encrypted traffic between PBXs -LDAP via TLS -SMTP / IMAP / POP3 connections over TLS -SSH console access -Intrusion detection over all services managed by the PBX (SIP / RTP / DNS proxy / NTP / Web) -DoS protection over all services managed by the PBX (SIP / RTP / DNS proxy / NTP /	https://wildix.atlassian.net/wiki/x/pQvOAQ, section "Security measures in place"

			Web) -SIP SBC built in -Protection against cross-site request forgery (CSRF) attacks	
	Are data copies (e;g. on development platforms) anonymised or pseudonymised?	N	Wildix does not make copies of user data	
Account and access management	Is there a documented user lifecycle management process in place?	N	Up to end-customer or Partner to implement this process (not performed by Wildix)	
	Is there a formal acces management process in place guaranteing that users are only granted the rights they need?	Y	Available in the main Wildix application, WMS, under "Users" (process is performed by the Wildix Partner, not by Wildix)	https://wildix.atlassian.net/wiki/x/8xrOAQ, section "Admin and Default ACL groups and permissions"
	Is there a consolidated view of all applications accesses and rights for each user?	Y	Available in the main Wildix application, WMS, under "Users"	https://wildix.atlassian.net/wiki/x/8xrOAQ, section "Admin and Default ACL groups and permissions"
	Are high privileged accounts managed specifically and their access rights limited?	Y	Available in the main Wildix application, WMS, under "Users" (access management is performed by the Wildix Partner, not by Wildix)	https://wildix.atlassian.net/wiki/x/8xrOAQ, section "Admin and Default ACL groups and permissions"

	Is the Group password policy applied?	Y	Minimum length and complexity requirements in place specifying a recommended length of 12 characters and at least one: -Capital letter -Special character -Number Password changes are recommended every 6 months, and account lockout is enforced for 1 hour after 3 unsuccessful access attempts	https://wildix.atlassian.net/wiki/x/pQvOAQ, section "Frequently Asked Questions," sub-heading "Access Control," column "What system enforced password settings are active for users?"
	Is there a secured password reset process?	N		
	Are end users regularly inform about security topics including GDPR?	N		
	Are specific IT populations (administrator, project manager...) trained on IS security policies?	Y	Technical training, including training on Wildix security policies and procedures, is required for all onboarded Wildix Partners.	
Infrastructure protection	Is the datacenter security level aligned with the application SLA?	Y	Wildix security measures are in alignment with security measures by AWS.	AWS: https://aws.amazon.com/agreement/ (section 3) Wildix: https://wildix.atlassian.net/wiki/x/8QvOAQ

	Is there an access control in place in the datacenter with logging of all entries?	Y	Datacenter is a non-descript facility which features: -Physical access controls, including physical barrier controls requiring access control validation -Limited employee and contractor access -Physical security protections, including locked entry doors, surveillance cameras and electronic intrusion detection systems	https://drive.google.com/file/d/1TJbv8N81RmYmKUaxYslCNF-0AQPvbRiA/view?usp=sharing, pages 7-8 (Annex 1, section 1)
	Is infrastructure segmented by zone and the segmentation compliant with usual corporate policies?	N	Infrastructure is not segmented by zone	
	Is there a formal flow matrix between these zones and a formal validation process for flow approval?	N		
	Is the filtering matrix implemented and verified in local FW?	N		
	Are network accesses to applications processing personal data encrypted using appropriate - non-vulnerable - protocols?	Y	Access to such applications is available only for the "super admin," the only user with full access to all levels of system management, and to users given access by the system admin; access is restricted by	https://wildix.atlassian.net/wiki/x/pQvOAQ, under section "Frequently Asked Questions," sub-header "Access Control," question "Which access methods are available to access the system?"

			user password login	
	Is the infrastructure hosting personal data and applications hardened , particularly by removing the unused services and disabling protocols not strictly necessary for the proper functioning of the application?	**Y**	Wildix Cloud services operate through data centers that are required to undergo and pass ISO 27001 audits, and personal data and related services are regularly deleted in accordance with GDPR standards.	https://wildix.atlassian.net/wiki/x/pQvOAQ, sub-heading "Wildix Cloud and ISO 27001 compliance" and "Privacy and GDPR Security"
	Is the infrastructure hosting personal data and applications updated regularly and contains no outdated components?	**Y**	Infrastructure updates are detailed on the "New Releases" page on the Wildix website	https://www.wildix.com/new-releases-and-updates/
	Is the infrastructure hosting personal data and applications protected by a supported and up-to-date antimalware solution?	**N**	Encryption methods and multi-tiered security are used in place of an external antimalware solution.	
	Has the infrastructure hosting personal data and applications no known critical vulnerability, detected through at least monthly vulnerability scans?	**Y**	Wildix manages vulnerabilities with the OWASP Risk Rating methodology and has SLA depending on the severity of security defects. Currently, we have no known security defects rated as High or Critical.	

	Is the infrastructure hosting personal data and applications regularly patched at least every quarter ?	**Y**	Infrastructure security fixes are typically deployed immediately after the relevant fix is ready and tested, and each application's auto-update is enabled by default. Security fixes are usually released as a hot-fix and available immediately after testing.	Summary of patches, including their frequency, can be seen for each application on the updates page: https://www.wildix.com/new-releases-and-updates/
	Are applications and data regularly backed up?	Y	Possible to schedule regular backups, but the process must be implemented by Partner or end-customer	https://wildix.atlassian.net/wiki/x/mBfOAQ, sub-heading "Backup system"
	Are backups encrypted and stored in a different location?	Y	Backup process is done at discretion of Partner or end-customer and security of backups is at their discretion	https://wildix.atlassian.net/wiki/x/mBfOAQ, sub-heading "Backup system"
	Are there periodic restorations tests (at least twice a year)?	Y	Using hardware or virtual PBXs (must be implemented by Partner or end-customer)	https://wildix.atlassian.net/wiki/x/mBfOAQ, sub-heading "Storages (Hardware, Virtual PBX)
Application protection	Are applications accessible from internet published through a DMZ?	Y	Applications can be published through a DMZ and achieve connectivity to external trunks and users depending on the individual configuration, but can also be used on isolated networks should all	

			connections and users be internal.	
	Are applications accessible from internet architectured with a 3-tier architecture?	Y	By default the application server and database are located on the same tier, but given a specialized configuration, the database may also be moved to the data management tier.	
	Is there a methodology to ensure quality and security of coding used? For web application, are the OWASP recommendations enforced??	Y	Wildix uses OWASP SAMM as the main methodology for implementing SDLC and follows the security practices recommended by this model.	
	Are all application components (middelware, database...) updated and in a suported version?	Y	New Releases and Updates page on website details changelogs for all supported Wildix applications	https://www.wildix.com/new-releases-and-updates/
	Are infrastructure and application vulnerabilites detected on a regular basis (recommended everymonth) and critical vulnerabilites fixed?	Y	Wildix expeditates the patching of any and all Critical defects in order to fix them ASAP. Vulnerability scans and penetration tests are performing regularly, and we implement continuous dependency tracking.	

Incident & crisis management	Is there a specific security incident process in place?	Y	Security incidents are handled after being reported either to security@wildix.com or the 24/7 NOC team included with Wildix Support	https://wildix.atlassian.net/wiki/x/8QvOAQ, support hours specified in section 2 ("Support Hours"), incident reporting process specified in section 3 ("How to interact with Support") and https://wildix.atlassian.net/wiki/x/pQvOAQ, sub-heading "security vulnerabilities report"
	Are the local CISO and the operational teams informed/trained on the management of security incidents (including the use of the Group incident response service)?	Y	All such individuals are trained to either contact the Wildix NOC team or submit vulnerability issues to the email security@wildix.com	https://wildix.atlassian.net/wiki/x/pQvOAQ, sub-heading "security vulnerabilities report," and https://wildix.atlassian.net/wiki/x/8QvOAQ, Art. 17, "How to interact with support"
	is there a formal review of security incidents and lessons learned identified and implemented?	Y	NOC team reviews causes behind any system crashes or security issues through logs after fixes are implemented, both to improve upon system architecture and communicate with any Partners who may have reported the problem in question.	https://wildix.atlassian.net/wiki/x/8QvOAQ, Art. 18.2
	Is there a crisis management process in place and tested annually?	Y	NOC team carries out extended support service for severe issues upon detection	https://wildix.atlassian.net/wiki/x/8QvOAQ, Art. 16.2, Art. 16.4-16.8.

Security monitoring	Are infrastructure and application logs collected and saved for at least 6 months?	Y	Logs are collected within a centralized system and stored anywhere from 2 weeks to a year depending on the severity of the issue in question.	
	Is the logging level set to allow collecting relevant security event as well as read and write access to personal data?	N		
	Is log correlation for incident detection implemented?	Y	NOC team analyzes logs from all systems and detects strange patterns indicating evidence of attack or fraud	https://wildix.atlassian.net/wiki/x/8QvOAQ, Art. 18, "Proactive system monitoring and crash reports"
	Are intrusion tests regularly performed?	Y	Penetration tests are performed yearly and security reports summaries are released on request after signing an NDA to existing customers.	https://wildix.atlassian.net/wiki/x/pQvOAQ, section "System Web Security", question "Are any vulnerability scanning or penetration testing carried out?"
Project management	Are personal data formally identified at the start of each project?	Y	Partners are trained with the expectation to identify these data as they begin each end-user's installation.	
	Is there a risk analysis done at the beginning of application projects?	N		
	Are there security reviews during application projects, specifically at the end of the design phase and at acceptance?	N		

	Is there an intrusion test performed before go-live?	N		