Supplier conditions and checklist

Universitair Ziekenhuis Brussel (UZB) is concerned about the stability and security of its ICT environment and about the availability, authenticity, integrity and confidentiality of the data of the hospital, its patients and employees. Therefore, the following describes what UZB expects when contractors or suppliers (both terms are used as synonymous with each other) want to implement a solution - an application, device, service, configuration, etc. - for UZB, regardless of the solution chosen or proposed

In an intuitive way, these expectations are explained in different sections each time in the left-hand column after which, in the right-hand column and in appendices, the contractor is given the opportunity to interpret its choices by providing additional information or proposing well-founded alternatives

You will find that UZB relies on industry standards and best practices for its expectations. It encourages suppliers to also use these standards as much as possible for their solution. After all, this increases efficiency for all parties involved - not only during the selection and implementation phase, but certainly also during the usage phase. In this way, you contribute to a stable and secure ICT environment. Staff and patients will thank you for this!

Finally, a timely and qualitatively completed checklist allows for a qualitative and smooth analysis by UZB, thus contributing to a good understanding about the solution(s) and the supplier and any risks associated with the solution(s). This in turn ensures effective selection and smooth implementation and cooperation in a good understanding.

If, while processing the checklist, you have additional questions or require clarification, please contact your contact person(s) at UZB who has been designated for this purpose. Important: always use the references in the first column for all your questions and attachments. Your contact person will also communicate to you the timings for receiving the completed document. It goes without saying that documents that deviate from UZB standards will require more analysis and consultation time.

Technological expectations

This section covers all technical aspects of the solution(s).

Frame

TK01	**Technological solutions**	Indicate here which solution(s) will be worked out by you in this document: client/server (on-premises in UZB's data centres), XaaS, ... If you work out different solutions, please mention here which one you prefer and why that is so.
TK02	**Equivalence of** solutions. If the supplier proposes different technological solutions,	Indicate here whether and how the solutions are equivalent or not.

	UZB expects all solutions to be equivalent in terms of functionality, technology, availability, integrity, confidentiality and privacy.	
TK03	**Support over time.** UZB expects proposed solutions and all its components to be sold for 5 years and supported for 10 years after purchase.	State explicitly here if and for which (parts of the) solution this is *not* the case.

Client

TC01	By default UZB procures, installs and configures all client **hardware**, client licenses and connected equipment	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TC02	UZB installs and configures its clients on the latest **Windows** release by default, either on physical client hardware or on a VDI solution. Updates are applied automatically and regularly.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. List here any restrictions to running software on vmware horizon.
TC03	Clients are installed with (one/most recent) version of this **software** by default: - Microsoft Edge & Google Chrome - Adobe Acrobat Reader - TrendMicro ApexOne Antivirus - Office 365 - .net and are configured, managed and updated by UZB. Remote monitoring and remote management software will not be allowed. Remote access can only be allowed after consultation with and agreement by UZB.	Other software with the same functionality will not be allowed. If the software and its management listed here is not desirable in the context of the proposed solution, is suspected to be problematic, or if specific configuration (such as antivirus exclusions and socket communication) is desirable, please describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. UZB only allows open java versions such as adoptium, amazon corretto or Microsoft java. We especially do not allow Oracle Java version after version 8 u202 & version 11.02 because they are paying.
TC04	Clients are by default joined in the **UZB-AD** domain and managed via GPOs.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative

		proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. Clients not allowed in the domain are put behind a network firewall.
TC05	Windows firewall is active on every PC, only for incoming traffic to the PC.	Describe port and protocol here if a port is to be opened.
TC06	Clients can be located in a separate VLAN. For peripherals, this is always the case.	In this context, describe the required firewall rules here. Add a Windows update policy or argue why this cannot be done.
TC07	**UZB prefers web-based applications. Additional software** required on the client as part of the solution is provided centrally and automatically to the client by UZB. Installation paths, file structure and disk layout are to be determined in consultation with UZB. **Software must be able to work without local-admin rights (nonnegotiable!) and must handle UAC.** Based on the agreements made, the supplier provides UZB with an MSI accompanied by the software installation manual as part of the as-built documentation.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. Provide the installation manual as part of the as-built documentation.
TC08	In UZB, **internet access** is linked to a user account. Service accounts do not have internet access by default.	If the application or peripheral requires autonomous internet access, this should be explicitly stated in the architecture documentation including the required firewall rules.
TC09	UZB has its own **Certificate Authority** (CA) that is automatically trusted by every device in the domain. This also applies to mobile devices. Certificates from the UZB CA must be used. This is particularly relevant for e.g. websites and not for devices communicating securely. In the latter case, e.g. for printers, self-signed certificates can be used.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. Specify here if a public certificate is required so that UZB can arrange this with an external CA (Sectigo).
TC10	UZB uses Exchange online as its **e-mail solution**. By default, unauthenticated e-mailing is impossible. Outgoing mail to the Internet is restricted to mail addresses with suffix uzbrussel.be. Other domain names are filtered by the mail gateway. If the application needs to be able to mail, there are 2 options:	Document the possible need for e-mailing here, including the required technical information. Describe here whether the solution is MS Exchange Online (o365) compatible. If non-authenticated: describe the IPs to be whitelisted here.

	a. Authenticated: via AD credentials with statement of mail addresses (preferred) b. Non-authenticated: IP address is added in an ACL on the load balancer and no check for mail address. For cloud applications via microsft graph api.	
TC11	**Access control** UZB prefers that on premise authentication is done via AD.	Describe here or in an appendix how access to the application will be set up on the client. Does the solution provide Role Based Access Control (RBAC)? What is the procedure for offboarding users?

Server

TS01	UZB expects to receive an **architecture design**: a clear diagram showing *all* components of the solution, information flows, IP addresses, protocols, ports and dependencies. Also include components that the solution uses, such as java, .net, web servers like nginx, apache, etc.	Document this in an appendix to this document. The design does not imply tacit acceptance but is the subject of consultation prior to any acceptance by UZB.
TS02	UZB does not use bare metal hardware for servers by default but offers **virtual servers** via VMWare vSphere and with underlying AMD Epyc CPU. All associated licences support HA, DRS & vMotion. Given its importance for regular hospital failover tests, vMotion cannot be questioned. Servers will be installed by UZB. Proprietary installations are only allowed for hardened solutions and are to be supplied in the form of an OVA/OVF meeting the conditions below. UZB almost always puts OVA solutions behind a network firewall due to update issues. OS installations via OVA/OVF should provide an admin account for UZ Brussel staff. *Black box* OVAs that cannot be logged on to the system are *not* accepted. UZB does not use nVidia GPU cards by default. If UZB agrees to install server hardware, it will be done by UZB, not in the active directory domain, in a separate network (VLAN) and behind a firewall.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. Specify explicitly whether VMWare Fault Tolerance is required. Specify explicitly whether nVidia GPU cards are required with the amount of RAM in GB, the number of desired CUDA cores as well as the type of licence for nVidia Grid and the desired profile.

TS03	UZB installs and configures its servers by default on the latest version of **Windows server, AlmaLinuxor RHEL**. Given the importance for information security, UZB will only allow an OS that is supported for at least 3-5 more years after purchase.	Document the desired OS here. Document here if the standard proposed options are not possible or desirable and describe the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB
TS04	Each server is always addressed within the provided application or peripheral via its Fully Qualified Domain Name (**FQDN**) with uzbrussel.be. Split DNS is used for FQDNs that must be available on the Internet	Indicate here whether split DNS is required.
TS05	Windows servers are members of the UZ Brussel **AD domain** uzbrussel.be and are managed via GPOs based on Microsoft secure baselines. These settings apply to all devices: i. Disable SMBv1 (Windows file sharing). SMBv2 is tolerated but not desirable. ii. Disable LM (LanManager) & NTLMv1. NTLM is being phased out in favour of windows integrated authentication via kerberos. iii. UAC active iv. Windows Firewall. TCP/UDP ports to be set up should be defined precisely. It is allowed to define any application in the Windows firewall. Only incoming traffic will be filtered. v. User Rights Assignment (Windows privileges) are only managed via GPO and cannot be controlled via a local GPO (e.g. act as part of the OS, logon locally rights etc) vi. SSL2.0, 3.0, TLS1.0 & 1.1 are disabled by default. vii. Connecting to AD is done only via LDAPS - not LDAP. viii. Credential guard is active by default. ix. Print spooler is off. x. No local users are created and accounts may not be added to the local admin group without explicit approval from UZB. In case of positive approval, this is done via an AD group and not directly in local groups. Servers that do not meet these conditions are removed from the domain and put behind a network firewall.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. List any Windows firewall settings here.

TS06	Servers are installed by default with **antivirus software** configured, managed and updated by UZB. Periodically, a full scan of the server is done that can affect performance. This is especially important for any socket-based communication. If this form of communication is used, it is to be explicitly stated in the design documents.	Indicate any scanning exceptions here. Indicate here any use of socket-based communication and any need for an exclusion list.
TS07	UZB autonomously, regularly and automatically **updates** the servers under its management. It does this in phases with a view to securing the network environment. Security updates must be allowed.	If this is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TS08	UZB installs 7zip, notepad++ and MS Edge by default. Any **additional software** to be installed on the server shall be prepared by the contractor in MSI format and accompanied by an installation manual. The installation of the software on the server should be agreed between UZB and the supplier. The contractor can install the software autonomously, but the software must always be checked by an employee of UZB before going into production. Any new versions/updates follow the same path. Services and tasks always run with an agreed service account **without** admin rights.	Describe here if/which software to install. Deliver msi and installation manual to the technical contact at UZB.
TS09	UZB makes a very explicit distinction between **installation/support accounts and service accounts:** i. The account provided for the installation and support of the application(s) is disabled after installation. This account may therefore not be used to run a service, create a database connection or mount a fileshare, for example. ii. Local system accounts are explicitly not allowed. A service account can be created by UZB if a service needs domain credentials instead of the default system account. This then becomes a Group Managed Service Account ***without admin rights*** whose password is managed by AD.	Describe here if and for what purpose/what rights (registry, configuration files, etc.) a service account is needed. Meet with the technical contact at UZB to share the service account password. If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.

	iii. Service account password must ***not*** appear in clear text visible in configuration files. Applications run in production as services without local admin rights - (local service or network service account are allowed). So a uzb ad account need not necessarily be used and if an AD service account is used then preferably MSA account and not a default AD account so that password rotation happens automatically. Contractors are not provided with the corresponding password. GUI-based executables (processes that cannot be started as a service) are not accepted.	
TS10	**Authentication** is done with Windows integrated authentication via Kerberos and possibly via NTLMv2 (no NTLMv1 or LanManager) AD LDAP authentication only via LDAPS and not plaintext LDAP.	If the UZB approach is not possible or desirable under the proposed solution, describe here the exact rationale with an exhaustive elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TS11	No server on the domain may be taken **over remotely** without prior consultation with UZB: i. During the project phase, a domain account is provided for the solution through which installations will take place. After the project phase, this account will be disabled. ii. To ensure the stability of the solution, the supplier can access the environment after the project phase according to the process UZB provides for this as standard and via a VPN Pulse Secure Client (via TOTP) in combination with a PAM solution. For this, the acquirer must install a plugin on her/his PC.	If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TS12	UZB **monitors** the entire server environment.	State here or in an appendix which services & URLs of the service are to be monitored, which thresholds apply and the interrelationship between the different services and the user experience.
TS13	UZB signs all necessary certificates internally with the UZ Brussel **Certificate Authority (CA)**, which is automatically trusted by every device in the domain, including centrally managed mobile devices.	Indicate here whether a public certificate is required. Include a subject & SAN names and what the certificate will be used for: server authentication and/or client authentication and/or other.

	The supplier uses certificates from the UZB CA. If a public certificate is required, UZB purchases it from an external CA.	
TS14	**Internet access** from servers or communication with specific public addresses on the Internet is not allowed.	If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. The proposal includes a detailed configuration of Windows firewall and network firewall. For applications that need to be available from outside, this includes details such as URLs, IP addresses, ports, protocols, etc. to enable this in a controlled manner.
TS15	**Non-encrypted, known insecure or outdated protocols** such as ldap, http, ftp and telnet are not allowed.	If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TS16	UZB **backs up** the systems under its management as follows i. Of virtual servers, 3 storage-level snapshots are taken every day where a crash consistent backup is taken. ii. Databases supported by UZB (see further "Database server" on this subject): For MSSQL, transaction backups are provided every 30 minutes.	If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB. If the supplier uses other DB systems, please refer to the relevant information under "Database server". In such cases, ICT will only provide a file-based backup of a database export provided by the supplier.
TS17	**Application data** is always stored outside the VM on a NAS location so that the VM does not become too large and storage can be adapted efficiently. UZ Brussel has a high-availability storage platform and long-term storage on archive for this purpose. Snapshots can be maintained for up to 3 years with copy on a tier2 disk array and an offsite copy on tier3 environment. All file serving/NAS needs should be foreseen on these pre-existing systems. If there is a limited amount of	State explicitly here if a separate backup retention policy is needed for application data.

	application data (< 50GB), it can be stored locally.	
TS18	**Creation and configuration of Local SMB/CIFS shares** on Windows servers are by default not allowed without UZB staff intervention	Specify explicitly here if and which local shares are needed. UZB creates these, taking into account the creation and application of AD groups and NTFS permissions. Specify which persons need access to the service (or service account(s).
TS19	For the use of e-mail, the same rules apply for servers as for clients: UZB uses Exchange online as its **e-mail solution**. By default, unauthenticated e-mailing is impossible. Outgoing mail to the internet is restricted to mail addresses with suffix uzbrussel.be. Other domain names are filtered by the mail gateway. If the application needs to be able to mail, there are 2 options: a. Authenticated: via AD credentials with statement of mail addresses (preferred) b. Non-authenticated: IP address is added in an ACL on the load balancer and no check for mail address For cloud applications via microsft graph api.	Document the possible need for e-mailing here, including the required technical information. Describe here whether the solution is MS Exchange Online (o365) compatible. If non-authenticated: describe the IPs to be whitelisted here.

Shared server infrastructure

UZB consolidates some core functions on central systems and strongly encourages suppliers to use them:

TG01	**Communication server** (**HL7 messages**) Communication of the solution with the central UZB systems is preferably over HL7 via Mirth. The supplier provides socket-based communication with Mirth. Alternatively, one or two shares are defined on the central storage platform or on (one of) the server component(s) of the application for inbound and outbound file-based communication.	Indicate whether the supplier wants to use socket-based Mirth communication or (a) share/s. If the UZB approach is not possible or desirable in the context of the proposed solution, describe here the exact rationale with an exhaustively elaborated alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TG02	**Database server** Microsoft SQL Server is provided and supported by UZB. The supplier is provided with one or more databases on the central SQL database server. UZB uses a central SQL 2022 enterprise edition for this purpose. i. UZB takes responsibility for licences, installation of the database (SQL script to be	Indicate whether/which of the central database solutions the supplier wishes to use. Specify the initial and expected database size. If other databases are required, the supplier will install and maintain them itself.

	provided by the supplier), for availability and for backup and restore of the environment. Any report services and other database activities (SSIS, SSAS, SSRS, ETL...) are performed from another server. For installation and any troubleshooting activities, the contractor will be provided with appropriate contacts. No sysadmin rights are granted to the vendor on the central MS SQL server. ii. The contractor responds promptly and efficiently when DBA analyses show that a particular query threatens system performance. By agreement, MariaDB can be offered centrally. Also Postgresql, but the latter not centrally. Oracle databases or products are not an option.	The supplier will update/patch the database software regularly and on its own responsibility so that security and stability remain guaranteed. The licence for this database is provided by the supplier. The supplier hereby takes into account that this database server runs on a vmware virtual platform which may have implications on licensing. Backup (scripts) must be provided by the supplier and backups must be stored in a location outside the server on a NAS. This NAS location is provided by UZ Brussel. Communication between application and database servers must be encrypted with TLS1.2 or higher If the contractor requires sql reporting services, the collation must be specified for MS SQL (if different from Latin1_general). If Oracle databases or products are required for the solution, the supplier must guarantee UZB with a certificate from Oracle that they can run on vmware (embedded Oracle licence). If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TG03	**Load balancer** To make a solution full tolerant and high available, UZB offers its NGINX software load balancer, HA Proxy or Reverse Proxy for those applications that can handle it	Please state explicitly here if and which of this solution you wish to use for this purpose.
TG04	**Fileserver** See above under "Application data"	-
TG05	**Web server**	i. Indicate here whether the solution uses a web server. ii. Indicate the subject and SAN names for which the certificate is used. See also TS13 on certificates.

As-a-service solution

TA01	UZB expects to receive an **architecture design**: a clear diagram showing *all* components of the	Document this in an appendix to this document. The design does not imply tacit

	solution, information flows, IP addresses, ports and dependencies.	acceptance but is the subject of consultation prior to any acceptance by UZB.
TA02	**Information security and privacy**. UZB expects the availability, authenticity, integrity and confidentiality of the data of the hospital, its patients and employees to be guaranteed at all times.	Describe here or in an appendix: i. Describe encryption of data in transit and at rest ii. Where will the data be kept - including backup. iii. At what frequency is the backup done, how long are backups maintained, what are the typical restore/RPO/RTO windows? iv. Who has access to UZB's data and with what roles and rights? v. Is permanent deletion of data possible? vi. Who owns the data collected and processed under the contract? vii. How is data integrity ensured during transfer ("in transit") and storage ("at rest")? viii. Is sensitive personal data anonymised or pseudonymised to comply with laws and regulations? ix. How does the supplier ensure that anonymised data cannot be re-identified?
TA03	**Access control.** Authentication in the application is preferably done via EntraID and not with local users in the application.	Describe here or in an appendix: i. Does the solution provide Role Based Access Control (RBAC)? ii. Is Multi Factor Authentication (MFA) supported, and if so, how? iii. Is Single Sign On (SSO) with EntraID (or other IdPs) supported, and if so, how? iv. Are SSO features compliant with security standards such as SAML 2.0 or OpenID Connect? v. The procedure for offboarding users.
TA04	**Availability and Continuity** UZB wants optimal solution availability at all times.	Describe here or in an appendix: i. What uptime does the supplier offer over the total solution? ii. Does the supplier have a documented disaster recovery plan for restoring service and data. If yes, please provide this in attachment. iii. With what regularity is the disaster recovery plan tested? iii. How is the solution secured against distributed denial-of-service (DDoS) attacks?
TA05	**Infrastructure security**	Describe here i. What measures has the supplier taken to secure the underlying infrastructure. Also

	UZB wishes to be assured that the infrastructure from which the solution is offered is secure	make this transparent in the architecture design (see above) ii. Where (in which data centre(s) the solution will be hosted. iii. How the solution offered to UZB is segmented into the different layers of the OSI model iv. Whether and which tools such as Key Management Services or threat detection the vendor uses.
TA06	**Third-party integrations**	Describe here and/or in an appendix i. how the solution technically integrates with third-party solutions ii. how API keys and other credentials are stored iii. how the supplier evaluates third-party solutions
TA07	**Data recovery post contract.** UZB seeks clarity on recovery of its data after contract termination	Describe here how this is typically done and what options exist. Also mention data transmission rates.
TA08	**Network security**	Describe here or in an appendix: i. What network security measures are in place to enable communication between cloud resources? ii. Does the vendor offer Virtual Private Cloud (VPC) or virtual networks to enable secure isolation? iii. Does the vendor offer a Web Application Firewall (WAF) for web facing services? iv. How is network traffic monitored for potential threats such as e.g. DDoS attacks?
TA09	**Data sovereignty and localisation**	Describe here or in an appendix i. Are there any specific data residency or sovereignty requirements that the supplier meets? ii. Is it possible to choose data centres in specific locations to comply with laws and regulations?

Solution-independent expectations

The measures below are UZB's expectations about the supplier and the solution it offers, regardless of the proposed solutions.

TO01	**Transparency**. UZB expects a transparent attitude from the supplier in terms of security. This includes notification by that supplier of security breaches and vulnerabilities in the hardware, software, configuration or services of the solution, as soon as possible after their identification.

TO02	**Auditing.** UZB expects the supplier to be open to audits by UZB or by a third party appointed by UZB for this purpose, always within the limits of agreements on scope, costs and timing. The supplier supports UZB in this, for example by providing access to relevant documentation, logs, personnel or infrastructure. The supplier is also available for ad hoc questions from UZB on specific aspects of the solution during the duration of the cooperation.
TO03	**Ethical hacking**. Solutions publicly available under the UZB domain are tested by ethical hackers on behalf of UZB. Vulnerabilities in the vendor's solution are communicated to it. UZB expects these vulnerabilities to be resolved without delay and also expects transparent communication about them. If a vulnerability can be found within the software placed under the management of the contractor, the corresponding bounty can be passed on to the contractor.
TO04	**Suitability of supplied software and runtime environments.** All software and runtime environments supplied by the supplier (java, .net, python, etc.) must be free of known security issues as described in CVE-entries, among others. Only supported versions of applications and runtime environments are accepted. For each software component, we expect a description of the version and ongoing warranty/support. It is up to the supplier to keep all software components up to date. UZ Brussel has a vulnerability scanner tool that will check this.
TO05	**Suitability of personnel.** UZB expects that all work on the solution by the supplier or by a party appointed by the supplier will be carried out by personnel who are suitable for this purpose. Suitability means (a) that these persons are technically knowledgeable about the solution and all components that form part of it; (b) that these persons comply with all relevant laws and regulations and UZB-specific instructions; (c) that these persons behave in a professional and ethical manner. UZB reserves the right to monitor this and to deny access to its systems or premises to persons who do not comply with one or more of these requirements.

TO06	UZB expects that **updates** to the solution i. can be performed as much as possible without downtime. ii. can always be rolled back.	Describe the solution's update mechanism here, including whether and how much time to foresee unavailability during an update. For DB integrations, UZB expects a script to roll back DB updates as well. This is part of the as-built file (see elsewhere)
TO07	**Securing unauthorised changes.** UZB expects the solution to be secured against unwanted and/or unauthorised changes to the hardware, software, or configuration of the solution	Describe here how the solution is protected against unauthorised changes.
TO08	**Security logging**. UZB expects the logging of mutations of data in the solution so that at any given time it can be found out who made what change when.	Describe the security logging of the solution here: what is logged where and for how long. Describe how UZB can access this without interacting with the contractor
TO09	**Errors and error detection.** UZB expects the solution to include a system for detecting and correcting errors in data input, processing, output and dissemination. This system includes means for verification of the completeness, correctness and authenticity of internal and external dissemination of data. The system also complies with the applicable guidelines at the	Describe here the means of detecting and correcting errors in data entry, processing, output and dissemination.

	time of use from government for, among other things, securing the information data.	
TO10	**Monitoring** UZB wants a regular overview on the health and safety of the solution.	Describe i. who (UZB/supplier) monitors which parts of the solution. ii. which parameters of the solution are typically and with what frequency monitored. iii. which logs are available out-of-the-box for monitoring iv. of logs can be integrated into UZB's Security Information and Event Management (SIEM) tool. v. whether logs are anonymised or not to protect personal data.
TO11	**Authentication - general** Authentication is done via AD or entraID i. Passwords are not stored with or in the solution. All passwords are securely shared with UZB to be stored in a password vault. ii. Generic accounts are not allowed; each user has a unique login/password combination. iii. When application logons are created, salting and hashing is mandatory.	UZB expects the list of accounts and passwords as part of the as-built file (see elsewhere) Passwords delivered to UZB in files must be encrypted and accompanied by instructions on how an update is possible.
TO12	**Authentication - Single Sign On (SSO)** UZB requires authentication at every startup of a multi-user solution and prefers solutions that integrate with Imprivata.	Describe the capabilities of SSO solutions and integration with Imprivata in particular.
TO13	**Authentication - Multi Factor Authentication (MFA)** UZB requires MFA for solutions made available to its users over the internet.	If the UZB approach is not possible or desirable under the proposed solution, please describe here the exact rationale with an exhaustively developed alternative proposal. This proposal does not imply tacit acceptance but is the subject of consultation prior to any agreement by UZB.
TO14	**Authorisation** i. UZB expects a clear overview of authorisation options in multi-user solutions. ii. User management is automated at most through Active Directory via Kerberos (preferred) or NTLMv2 - i.e. without manual intervention for creation, changes and termination of users. iii. access management and role assignment are at least linked to the UZB AD via Entra ID. iv. Naming will be agreed with UZB in advance.	In case of multi-user solutions, describe here the types of users and (the content/scope of) their rights (read/add/change). Describe here the alternative approach for (parts of) multi-user solutions that cannot be automated via Active Directory.

	v. UZB expects authorisation to be via secure connections to Active Directory.	
TO15	**Incident response plan** **UZB** expects the vendor to have an up to date incident response plan that has been trained to its employees and users of the solution.	Describe the incident response plan here and/or attached. Describe here how customers are informed about a security incident. List here the significant security incidents the supplier has faced in the past 12 months. These are incidents with a real or potentially high impact.
TO16	**Application security** UZB expects that the solution was developed based on secure development best practices. UZB reserves the right to have its own solution pentested by ethical hackers. If serious defects are found, the costs may be recovered from the supplier.	If the supplier has developed the application itself, describe here i. Whether and which secure development best practices the supplier follows ii. Whether and how the supplier conducts regular code reviews iii. Whether and how often penetration tests are performed on the solution. - If yes, please provide us with the report on the most recent test iv. Whether the supplier uses a bug bounty programme. v. with what regularity the supplier releases security patches and updates vi. How quickly the vendor addresses vulnerabilities.
TO17	**Manuals**	Provide manuals for administrators and users.
TO18	UZB expects the supplier to inform the contact person at UZB as soon as the configuration or installation is completed - even if temporarily, e.g. when waiting for partial deliveries - and in any case before the commissioning of the configuration or installation in UZB's production environment. UZB expects to receive the following information within 4 weeks of completing the installation and configuration: **i. as-built file**. This is a faithful representation of installation and configuration as left by the supplier. ii. **verification procedure after patch/reboot**. This short document provides the checkpoints that UZB can use to verify the availability of the solution after patching or rebooting the system. The delivery of these documents may be a condition for any final instalment payment.	The documents are delivered via e-mail to the project manager and the technical contact at UZB.

Supplier expectations

This section addresses all the non-technical expectations UZB has about the solution and its supplier.

Licensing model

LL01	GENERAL. Describe exhaustively the **licensing model** of the solution(s).	Provide here or attached a list of all components of the solution and how and by whom they should be licensed. Here, also clearly indicate licences of any OS, DB & other supporting products or for all necessary modules within the package. Keep in mind active/passive environments, transfer of licences, etc. Given UZB can rely on its own contracts to provide licences, they are not an enforceable part of the solution. Provide proof if licence(s) are provided as a package under OEM by the supplier. Indicate whether academic licensing is possible. In doing so, also transparently describe the cost of all licences for all possible scenarios.
LL02	**Period of validity** of licence(s). UZB expects the validity period of the licence(s) to be in line with the expected lifetime of the solution.	Describe how long the licence(s) remain valid; how/when and by whom they are activated; grace period; ...
LL03	Is the licence enforced by **hardware solutions** such as keys & dongles?	If yes: describe.
LL04	Are **specific properties** such as MAC address or VM Hardware ID required?	If yes: state *for* implementation
LL05	UZ Brussel **only** wishes to licence **the production environment**. Can systems that do not belong to this environment be licensed?	If yes: describe.

Business considerations

Important: These questions should *not be* answered as part of a tender where they are already included in this process.

LZ01	UZB seeks clarity on the **contracting party**.	i. Indicate here which is the contracting party (name/seat). ii. Indicate here whether and which subcontracting party or parties the supplier wishes to use (name/seat).

LZ01	UZB wishes to cooperate with **financially sound organisations**.	Provide attached a recent financial statement of the organisation that will act as contractor.
LZ02	**Reference customers**	Provide the contact details of 3 reference customers who can be contacted by UZB independently of the supplier in the context of a possible collaboration.
LZ03	UZB seeks **contractual clarity**	Document a list here and provide attached a full set of *all* type documents (such as contracts, SLA, data processing agreement) that could be negotiated and signed at a contract stage. Important: this includes documents that are tacitly approved by signing a contract.
LZ04	**Compliance and certificates**	Provide here a list of all for-this-cooperation-relevant national and international legislation, regulations and standards with which supplier is compliant, including the scope for compliance. Explicitly state the applicable guidelines with which the solution provider is *not compliant*. Also include technically relevant standards such as about AWS, Azure and Google Coud. UZB reserves the right to also query the certificates themselves and the accompanying audit reports.
LZ05	**Financial overview**	Provide here or attached a list of all services or interventions for which supplier provides a cost to UZB.
LZ06	UZ Brussel **Privacy Policy**	Confirm that you have taken note of the UZ Brussel privacy regulations and as a supplier will also comply with these regulations. (To be found on the UZ Brussel website)
LZ07	**GDPR** - processing contract	In case personal data is processed within your solution, and a processing contract has not yet been drawn up, justify why you do not consider it necessary.

Contact information supplier

Contracting organisation	Name, address head office
Commercial contact	Name, phone, e-mail, date
Technical contact	Name, phone, e-mail, date

By submitting this completed form to your contact at UZB, you declare that you have taken note of UZB's expectations, understood them, and interpreted them to the best of your expectations and ability.

Incomplete and/or untimely forms may result in delayed analysis of the information and implementation of the solution up to and including exclusion from the selection process.