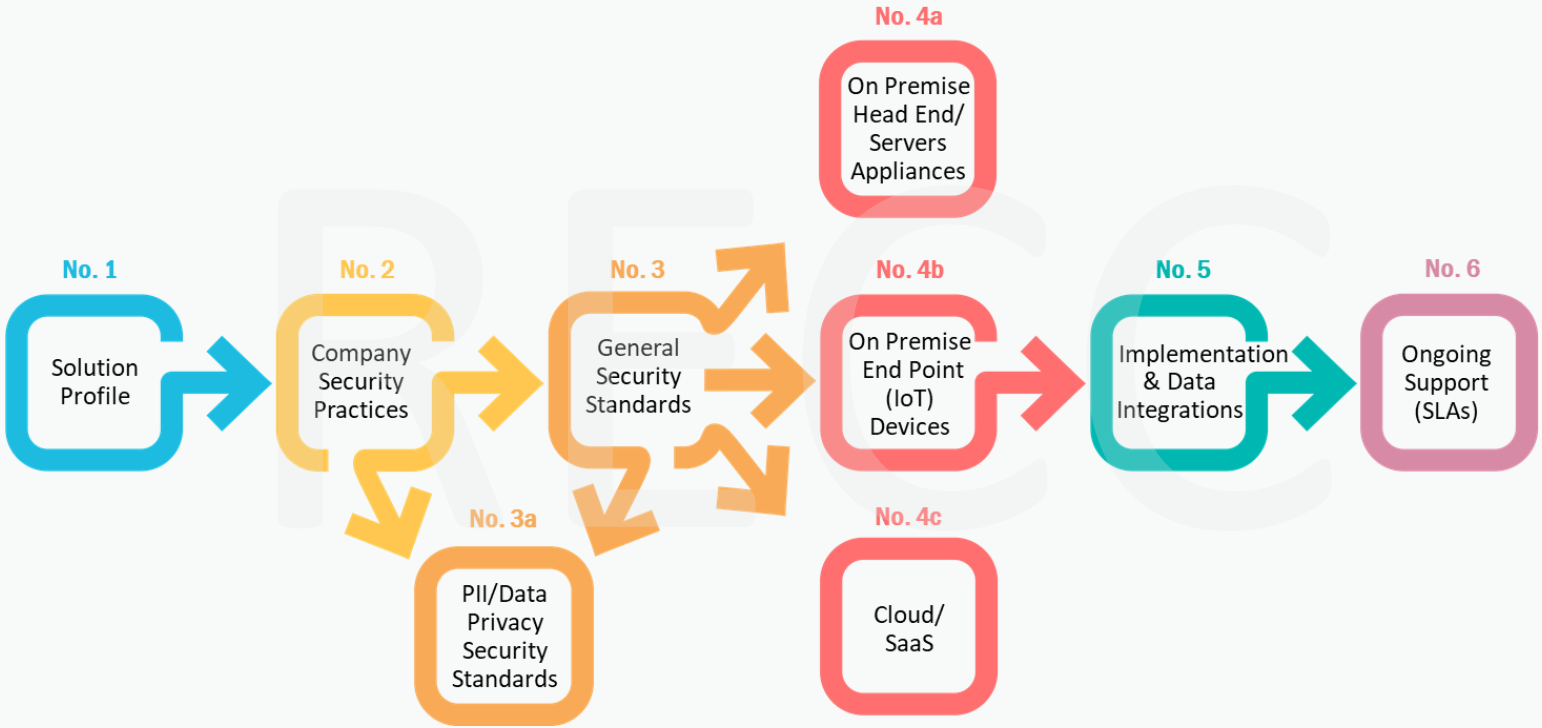
IT Security Assessment for OT Systems

Version 1.0

REAL ESTATE CYBER CONSORTIUM
(RECC)

REAL ESTATE
CYBER CONSORTIUM

IT SECURITY ASSESSMENT FOR OT SYSTEMS



REAL ESTATE CYBER CONSORTIUM

Overview

- General Solution Description
- Logical & Physical Design
- Current Release Version
- Underlying Database
- Supported Browsers
- Required Client SW
- Required Plug Ins
- Mobile Apps/Supported Devices
- SW Licensing Model

1. Provide an overview of the systems and services that you are providing.
2. Describe and illustrate the logical and physical architecture of your solution.
3. Which platforms (PC, Mac, mobile, etc.) are supported by your solution?
4. Describe the supported browsers and versions.
5. Does your software depend on any 3rd party plug-ins or applications to be loaded on your workstation (i.e., ActiveX, flash, java)? If so, please provide context.
6. What system and end user documentation is available?
7. What is the frequency of new software releases ?
8. Do you have a testing environment for client testing?
9. How long are clients given to test new releases prior to publication?
10. Provide the latest release notes and significant open bug listing.
11. What are the licensing requirements for your application?
12. What type of network connections and minimum bandwidth are required?
13. How is physical access to your data centers, computer rooms and data media storage areas controlled?
14. Do you provide software development and customization services?

Overview

- Employees-Contractors Background Checks
- Annual Acknowledgement of Security Policies
- Annual Formal Security Awareness Training
- Risk Management Program
- Cyber Insurance Policy Coverage

1. Does your company conduct both criminal and financial background checks for all employees who have access to nonpublic personal information?
2. Do you have a documented information security policy incorporating data protection methods, risk assessment, patch management, incident response, etc.? If so, please provide a copy.
3. Do you have a formally tested Business Continuity Plan?
4. Do you perform attack and penetration testing? If yes, is it performed by an outside 3rd party and what is the frequency? Which locations are covered by these tests?
5. Do you have a data / document retention policy? If yes, please provide.
6. Have you experienced any prior data breaches? If yes, please provide additional information.
7. Are you amenable to an on-site visit or 3rd party to access your data center for the purpose of confirming that the controls and security measures represented are in place?
8. Are employees and consultants that have access to nonpublic personal information trained on how this information should be treated?

Overview

- Account & Password Controls
- Windows AD Integration/SSO-SAML Integration
- Multi-Factor Authentication
- Logging
- Encryption Support
  - Browser
  - Data Transmission
  - At Rest

1. Describe your system's capabilities around single sign-on (SSO), federation and multi-factor authentication (MFA), and support for 3rd party clients.
2. How is software development handled (i.e. in-house resources, external sub-contractors, 3rd party developers? In what countries are they located)? How do they attach to your corporate networks?
3. Describe the security controls and encryption available in your application(s) (i.e. SSL, TLS, AES-128).
4. What specific TCP/UDS ports does your application use? Can these ports be changed?
5. How do your software development resources access your corporate network and code libraries?
6. Ability to verify Process Integrity: Verify that handling and processing of information is properly tested and controlled, including monitoring and control of physical and logical access and manipulation of data.
7. Ability to verify Confidentiality: Verify that protection of all client data at all phases of implementation and production, including monitoring and control of access by both internal and external parties.
8. Do you conduct stress testing on the product? If so, provide an overview of the process.
9. Do you provide user activity reporting (i.e. Users added, login failures, etc.)?
10. Does the product provide an audit trail of login attempts / failures/ and changes to configuration settings?
11. Describe your data at rest and data in transit protections.

PII/DATA PRIVACY SECURITY STANDARDS

Overview

- Privacy Policies
- Acceptable Use Policies
- Data Compliance Regulations
  - US
  - Canadian
  - GDPR
  - CCPA

1. How is personally identifiable information (PII) or personal financial information (PFI) stored, maintained and accessed?
2. Do you have a company data (including consumer data, HIPAA, PCI/PA-DSS) privacy policy?
3. Does your organization store and / or replicate data outside the US? If yes, what countries?
4. If data is stored in Europe does your organization comply with GDPR?
5. If data is stored or replicated in Canada does your organization comply with the Canadian Data Privacy Laws? (PIPEDA, PIPA Alberta, PIPA BC and Quebec Privacy Act)
6. Will your organization be compliant with the California data protection laws going into effect in 2020?

ON PREMISE HEAD END/SERVERS-APPLIANCES

Overview

- Hardware Requirements
  - Applications Servers
  - Database Servers
  - Clients
- OS+ Batch Management
- IoT Standards

1. What are your minimum and recommended hardware requirements for: Application Servers?
2. What are your minimum and recommended hardware requirements for: Database Servers?
3. What are your minimum and recommended hardware requirements for: Workstations?

ON PREMISE END POINT (IoT) DEVICES

Overview

- Hardware Requirements
  - Applications Servers
  - Database Servers
  - Clients
- OS+ Batch Management
- IoT Standards

1. What are your minimum and recommended hardware requirements for: Application Servers?
2. What are your minimum and recommended hardware requirements for: Database Servers?
3. What are your minimum and recommended hardware requirements for: Workstations?

Overview

- Cloud/Hosted Provider
- Cloud/Hosted Location(s)
- Certifications (SSAE18, SOC 1-2)
- Design including Backup
- Breach/Compromise Notification Process
- Defined Maintenance Windows
- Disaster Recovery Plan/Annually Tested
- Vulnerability Management/Scanning
- SLA Credits

1. If the solution is hosted, where are the hosting facilities located and who is the hosting provider?
2. Does your hosting facility have an SSAE18 report? If so, please describe the type of report (e.g., SOC 1, SOC 2, SOC 3, Type 1, Type II, etc.), the period of time covered by the most recent report, the firm that performed the most recent report.
3. Is this application hosted in a shared web or multi tenant environment? If so, what controls are in place to ensure segregation of client data?
4. Are all of your locations and service providers where client data will be housed or processed included in the scope of SOC 1 and/or SOC 2 examinations?
5. Do you perform internal and external vulnerability scanning? If so, what is the frequency and which product(s) or provider(s) do you use?
6. Describe the system redundancy, failover and disaster recovery plan. How often do you test your disaster recovery plan?
7. Do you have a formal breach notification policy?
8. Do you offer a high availability solution?
9. Ability to verify completeness: Certify that all vendor locations and service providers where client data will be housed or processed are included in the scope of SOC 1 and/or SOC 2 examinations.

Overview

- Data Migration
- API Design/Import-Export
- End of Term Data Migration

1. What are the available migration tools, either direct or third party, to assist in conversion/migration?
2. Do you provide standard APIs for both import and export of data from your system? Please provide a copy of your detailed API documentation.
3. What is your application and data integration architecture standard (SOAP, REST, others)?
4. Can we add or modify database objects such as triggers, views, indexes?
5. What is the underlying database/RDBMS for the application?

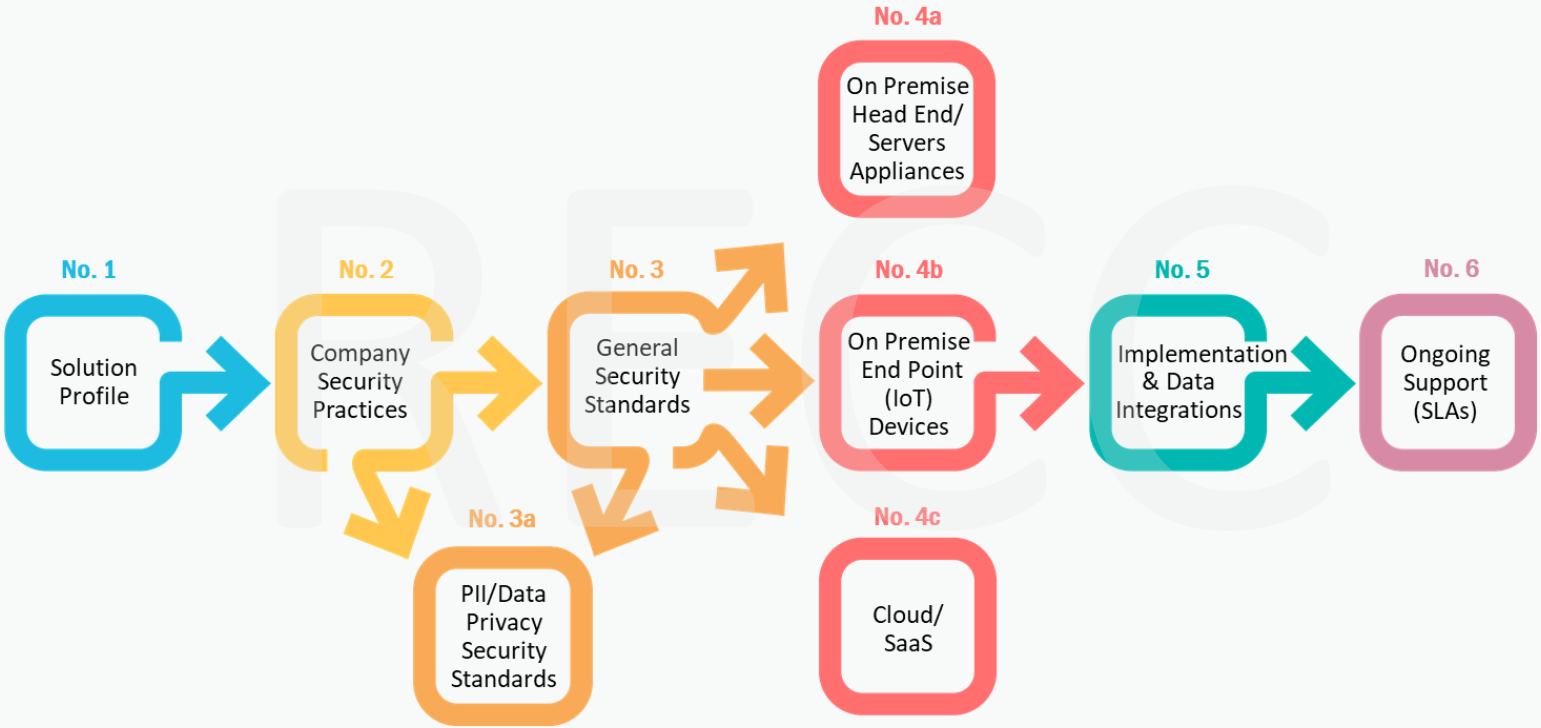
ONGOING SUPPORT (SLAs)

Overview

- SLA
- Support Hours
- Support Access
- New Release Frequency/Major-Minor
- Availability of Test Environment
- Change Management Policy
- Source Code Protections

1. What is your capability for a client to make, copy, and refresh environments (e.g. refresh the test environment with production data)?
2. Please describe your standard maintenance windows. Does the client have the ability to modify or limit these maintenance windows during normal operations and period close operations?
3. Please describe the application monitoring and notification capabilities provided with your solution. How do you ensure uptime?
4. Please outline client's capability to monitor or receive system performance notifications, benchmarks and actuals.
5. What do your Service Levels Agreements (SLAs) state in regards to system availability?
6. What are the application support models and hours of operation (Include reference to time zone)?
7. Is Source Code available for extensibility purposes? If so, please define.
8. Is the source code escrowed? If so, with whom and where?
9. How do you support operating system security or service pack patches / upgrades? What is your SLA related to security patches (timing after released from Microsoft)
10. Do you have an established Change control program?

IT SECURITY ASSESSMENT FOR OT



REAL ESTATE CYBER CONSORTIUM

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

Real Estate Cyber Consortium (RECC) ("Consortium") standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While the Consortium administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

The Consortium is a volunteer professional organization with no regulatory, licensing or enforcement power over its members or anyone else. The Consortium does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public because its works are not obligatory and because it does not monitor the use of them.

The Consortium disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. The Consortium disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. The Consortium does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, the Consortium is not undertaking to render professional or other services for or on behalf of any person or entity, nor is the Consortium undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

The Consortium has no power, nor does it undertake to police or enforce compliance with the contents of this document. The Consortium has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. The Consortium does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document should not be attributable to the Consortium and is solely the responsibility of the certifier or maker of the statement.

PRIVILEGED AND CONFIDENTIAL

Real Estate Cyber Consortium (RECC) ("Consortium") board members and contributor members ("Participants") are expected to ensure their participation and communications serve the procompetitive objectives identified by Consortium and do not violate the antitrust laws. Participants should focus discussions on Consortium's statement of articulated objectives.

This means that no activity or discussion at our meetings or other functions, or independent of our Consortium activities, may be engaged in for the purpose of bringing about any understanding or agreement among the Participants' activities that affects competition among the Participants including any of the following: (a) raising, stabilizing, or setting prices for products and/or services of the Participants; (b) regulating the nature or volume of products or services offered by the Participants; (c) allocating geographic markets or customers served by the Participant; (d) encouraging boycotts or unreasonably seeking to exclude specific entities and/or third-party vendors from the Consortium; or (e) otherwise restricting competition among the Participants and/or among third-party vendors.

In addition, Participants must not discuss or reveal any individual Participant's competitively-sensitive proprietary information, including any Participant's prices, margins, discounts, costs, capacity, inventory, sales, customer lists/customer contacts, future business plans, or bids for contracts.