# Project Details:

| | | | |
|---|---|---|---|
| **Project Name :** | | | |
| **Project Brief Description:** | | | |
| **Project Manager:** | | **Email:** | |
| | | **Contact Number :** | |
| **System Business Owner:** | | **Email:** | |
| | | **Contact Number :** | |
| **Vendor Details:** | | **Email** | |
| | | **Contact Number :** | |

## Instructions:

1. Below are the Information / IT Security requirements. Please answer all the questions. Incomplete forms will be rejected.
2. Please provide supporting document(s) -project scope, project charter, network diagram, ip addresses, required ports, hostname and encryption documentation (if encryption is used) etc.
3. Comments can be inserted in the REMARKS column in response to each baseline requirements.
4. If the answer is “Not Comply” or “Not Applicable” must provide justification at the justification column and submit risk management document (risk identification, assessment with mitigation plan) for “Not Complied” controls.
5. Please fill up the compliance percentage.
6. Project team will provide evaluated document during RFQ to Network Security & Audit team. Network Security & Audit team will verify and feedback.
7. Project Manager must ensure that all complied controls are implemented within the project, if any complied control found not implemented within the product lifetime concern vendor is solely responsible to remediate/implement the control(s).
8. Vendor will ensure all complied controls are implemented and provide certificate of those implementation.
9. Project team will provide signed Information Security Checklist to stake holder and Network Security & Audit during handover of the project.
10. Without information security controls implementation and signed information security checklist (filled up) will be considered as incomplete project/task.
11. Please check with Securitysense Network Security & Audit team if you are not sure how to fill up this document.

12. Securitysense Network Security and Audit team reserves all the rights to verify any system any time for Security Compliance.

## Background Information

| Serial # | Description | Response | Remarks |
|---|---|---|---|
| 1 | Where will be the server(s) located? | ☑ Pubail Data Center<br>☐ Uday Data Center<br>☐ Kaderia Data Center<br>☐ Mascot Data Center<br>☐ Hosting Company<br>☐ Vendor Company<br>☐ Others, Pls Specify: | |
| 2 | Expected functionality of the system (in brief) | . | |
| 3 | Number of infrastructure component (Network, Servers, etc.) | | |
| 4 | Who will be responsible for hardware & software maintenance? (please provide full details) | Hardware:<br>☑ Vendor<br>☐ Robi<br>Software:<br>☐ Vendor<br>☑ Robi | |

## Section A : General Controls

| Serial # | Description | Response | Justification | Remarks |
|---|---|---|---|---|
| 1. | Project Manager, Vendor need to ensure to comply with all information security policies and Procedures. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable<br>☐ Not Applicable | | |

| | | | | |
|---|---|---|---|---|
| 2. | All default account of the system/database/application must have to be disabled /locked before the service going to live. | ☑ Comply<br>☐ Not Comply | | |
| 3. | Restriction of application bypass: If a user connects to the database and bypasses the application, enforce security regarding this. There must be some mechanism to protect from such occurrence. | ☑ Comply<br>☐ Not Comply | | |
| 4. | Static IP address uses in application for scripting are not allowed. | ☐ Not Applicable<br>☐ Comply<br>☐ Not Comply | | |
| 5. | The Servers must be security hardened before going live by the corresponding OS's native hardening tools (e.g. Solaris JASS Script) and hardening document shall be handed over to the operation team. | ☑ Comply<br>☐ Not Applicable<br>☐ Not Comply | | |
| 6. | Test Platform may co-exist with Development platform but Test/Development platform must be isolated from production platform. | ☑ Comply<br>☐ Not Comply | | |
| 7. | Securitysense Information Security team will scan systems with scanning tools before Live. The scanned result must be satisfactory. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 8. | There shall be no limitation for conducting penetration testing and vulnerability assessment on the system / database / application. Securitysense Information Security (Network Security & Audit) will test anytime without any notification. | ☑ Comply<br>☐ Not Applicable<br>☐ Not Comply | | |

| | | | | |
|---|---|---|---|---|
| 9. | Vendor must have facilities / support to reduce the vulnerability and threat detected by Scanner or any tools. | ☑ Comply<br>☐ Not Comply | | |
| 10. | The systems must be protected and updated with standard antivirus software to protect any malicious attack. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 11. | Default Accounts like “Admin” or “Administrator” with Administrative privileged should be avoided in the system/database/application. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 12. | PING cannot be a way of monitoring or heartbeat between two hosts. So, others forms of monitoring criteria except ICMP have to use. If the service is published to Internet, ICMP service must be disabled. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 13. | Project Manager must consult with associate team for Database selection or design, hardware design and hardware placement in data center issue in the beginning of project. | ☑ Comply<br>☐ Not Comply | | |
| 14. | Project Manager will ensure to implement respective security policy/guideline/procedure (OS, application, database and Network etc.) in the system. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| | | ☐ Not Applicable | | |

| Compliances | |
|---|---|
| Total No of Compliance (Comply) | **13** |
| Total No of Not Compliance (Not Comply) | **1** |
| Total No of Not Applicable (Not Applicable) | **0** |
| **Presentence of Compliance:** ((Total Number of "Comply + Not Applicable" / 14) x 100%) | **92.86%** |

*__Note__: Please fill up the No. of **Comply/Not Comply and Not Applicable** fields then right click on the **percentage of compliance** field and click update, the % will be calculated automatically.

# Section B : Network Security Controls

| Serial # | Description | Response | Justification | Remarks |
|---|---|---|---|---|
| 1. | Perimeter devices (, Switch, ) must be configured as per security policy/guideline/procedure. | ☐ Comply<br>☐ Not Comply | | |
| 2. | All incoming or outgoing communications to External/Public Sites must go thru a staging server or via web server. The staging server must be located at the DMZ and only DMZ is allow to communicate to outside. The external communication should not be directly to/from the application or database server. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No server will be published in internet/DMZ | |
| 3. | If the service is published in Internet, the front end server must have to place in firewall DMZ zone and the application access from Internet must be through a DMZ reverse proxy. Inside Firewall access from Extranet shall not be allowed and Vendor shall provide necessary solution to achieve this requirement. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No server will be published in internet/DMZ | |
| 4. | The front end to back end communication (Between DMZ and Inside network) should be through FQDN or DMZ mapped IP address using only required ports. Inside IP segment will never be published to DMZ. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No server will be published in internet/DMZ | |
| 5. | If vendor requires remote access to the server to provide operation and maintenance or application support, the access should be through VPN connection. Securitysense Securitysense will provide necessary VPN client support to the vendor. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No remote Connection required for maintenance. Support will be ensure on site | |

☑ Not Applicable

| | | | | |
|---|---|---|---|---|
| 6. | There must have a network security architecture design indicating operational connectivity with every server in port level. The security architecture design must be approved by Information Security (Network Security & Audit). | ☑ Comply<br>☐ Not Applicable<br>☐ Not Comply | | |

| **Compliances** | |
|---|---|
| Total No of Compliance (Comply) | **2** |
| Total No of Not Compliance (Not Comply) | **0** |
| Total No of Not Applicable (Not Applicable) | **4** |
| **Percentage of Compliance:** ((Total Number of "Comply + Not Applicable" / 6) x 100%) | **100.00%** |

*__Note__: Please fill up the No. of **Comply/Not Comply and Not Applicable** fields then right click on the **percentage of compliance** field and click update, the % will be calculated automatically.

# Section C : System Security Controls

| Serial # | Description | Response | Justification | Remarks |
|---|---|---|---|---|
| 1. | The Operating System (OS) has to be configured or harden to meet Securitysense's OS security guideline. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 2. | By default all unwanted services must be closed. Only required services such as the client-server services, application services and system requirement services are allowed. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 3. | Disable all unneeded communication ports/services, program, removable media drive. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 4. | Warning statement on misuse of the system information and facility should be placed upon successful log-in or before log-in to the system. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |

☐ Not Applicable

| | | | | |
|---|---|---|---|---|
| 5. | Data dictionary should be used to document, standardize and control the naming convention and usage of data. | ☑ Comply<br>☐ Not Comply | | |
| 6. | The development, DR and production environment should be separated | ☐ Not Applicable<br>☐ Comply<br>☐ Not Comply | DR/Development platform is not incuded with this project scope | |
| 7. | System Partitioning: Does the solution use system partition where it allows scalable-processing or multi-processor and more than one application reside & share the firmware in a same physical box? | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No virtual environment /Stand along physical server. | |
| 8. | If partitioning of the applications is at the data-storage (LPARS), partitioning segregation or control mechanism must be in-place. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No virtual environment /Stand along physical server. | |
| 9. | If partitioning takes place at the physical-memory (memory addressing stack), control mechanism against risk of cross-addressing (e.g. in a memory-overflow) must be addressed. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | No virtual environment /Stand along physical server. | |
| 10. | System must be equipped /installed with latest patches available. | ☑ Not Applicable<br>☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | Tomorow |

| | | | | |
|---|---|---|---|---|
| 11. | Vendor shall provide documentation detailing all applications, utilities, system, services, script, configuration files, databases, and all other software required and appropriate configuration, including revisions and/or patch levels. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | OS version, kernel, Cluster suit |
| **Compliances** | | | | |
| Total No of Compliance (Comply) | | | | **7** |
| Total No of Not Compliance (Not Comply) | | | | **0** |
| Total No of Not Applicable (Not Applicable) | | | | **4** |
| **Percentage Compliance:** ((Total Number of "Comply + Not Applicable" / 11) x 100%) | | | | **100.00%** |

*__Note__: Please fill up the No. of **Comply/Not Comply and Not Applicable** fields then right click on the **percentage of compliance** field and click update, the % will be calculated automatically.

# Section D : ID Security (OS, Application & Database) Controls

| Control # | Description | Response | Justification | Remarks |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1. | Ensure the password related controls must be inbuilt in all systems (OS, Application, Database and network level):<br>a) Each user must have individual username and password. Password cannot be shared with others in any instance.<br>b) Minimum password length is 8 characters.<br>c) Force users to change temporary password at the first log-on.<br>d) Passwords contain combination of minimum three out of these four: one numbers, one capital character, one small letter, one special character (e.g.,!,?, #, %, *).<br>e) User cannot use the same password after next two times. (System will remember last two passwords).<br>f) Passwords are displayed on the screen in asterisk (*) form when being entered.<br>g) In network environment, users need to change password after 45 days interval.<br>h) Allow users to change their own passwords and include a confirmation procedure to allow for input error. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |

| | | | | |
|---|---|---|---|---|
| 2. | For secure authentication practice, the following security measures must be inbuilt install systems (OS, Application, Database and network level):<br>a) Systems or database or applications do not display the contents until the log-on process has been successfully completed.<br>b) System or database or applications authentication is transferred in encrypted from rather that clear text.<br>c) Upon completion of all input of log-in requirements, system validates the logon information. If errors arise, the system does not indicate which part of the data is correct or incorrect. Unsuccessful log-on attempts is allowed only to five attempts.<br>d) Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.<br>e) Display date and time of previous successful log-on and display details of any unsuccessful log-on attempts since the last successful log-on.<br>**f) As a security measure, after 30 minutes of no activity, log-on session automatically expires** | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 3. | Application, OS, and Database must ensure that the password MUST NOT be same as the user id or “PASSWORD” upon creation of the new user id. | ☑ Comply<br>☐ Not Comply | | |
| 4. | Vendor cannot have administrative password to work in the system/servers either locally or remotely after project go-live. If they require administrative password, that must be entertained and shall be attendant by a Securitysense system Administrator. In case of requirement to work from remotely a secured method shall be applied in this case | ☑ Comply<br>☐ Not Applicable<br>☐ Not Comply<br>☐ Not Applicable | | |

| | | | | |
|---|---|---|---|---|
| | (e.g. WebEx Session, Secured Shared Shell session etc). | | | |
| 5. | The input field for password MUST NOT visible while the users type in their passwords. | ☑ Comply<br>☐ Not Comply | | |
| 6. | Password MUST NOT stored in clear text. It must be encrypted or masked. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 7. | User id/Password repository (e.g. a file, database-table) MUST NOT be allowed to be copied out or must be secured against password-cracking. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 8. | Password must never be hard-coded into software developed. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 9. | System is able to generate alerts for failed login attempts (configurable) | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 10. | Account lockout must be configured. After 5 times of unsuccessful attempt, the user id will be locked. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |

☐ Not Applicable

| | | | | |
|---|---|---|---|---|
| 11. | Changing of password can be done without administrator assistance. | ☑ Comply<br>☐ Not Comply | | |
| 12. | IDs that have been dormant or inactive for 120 days must be revoked. Dormant period can be configured. | ☐ Not Applicable<br>☐ Comply<br>☐ Not Comply | Technically not possible in os level and no user exisit in application except application administrator | |
| 13. | Inactive ID for more than 120 days must be highlighted. | ☑ Not Applicable<br>☐ Comply<br>☐ Not Comply | Technically not possible in os level and no user exisit in application except application administrator | |
| 14. | Vendor supplied default passwords for the system should be changed immediately upon installation. | ☑ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 15. | Application provider will assist Securitysense to establish user access matrix. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |

| **Compliances** | |
|---|---|
| Total No of Compliance (Comply) | **11** |
| Total No of Not Compliance (Not Comply) | **0** |
| Total No of Not Applicable (Not Applicable) | **4** |
| **Percentage Compliance:**((Total Number of "Comply + Not Applicable" / 15) x 100%) | **100%** |

☐ Not Applicable

*__Note__: Please fill up the No. of **Comply/Not Comply and Not Applicable** fields then right click on the **percentage of compliance** field and click update, the % will be calculated automatically.

## Section E : Operation Security Controls

| Serial # | Description | Response | Justification | Remarks |
|---|---|---|---|---|
| 1. | System/Application/Database must have a backup mechanism to comply Securitysense Securitysense Standard backup and disaster recovery procedure to satisfy business continuity requirements. | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 2. | Project Manager to need consider redundant system for service availability | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 3. | Project Manager must ensure system must be compatible with Securitysense existing and future planned backup system.Also ensure system must be capable to backup from the 1st operation day. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |
| 4. | New system must have tape backup facilities and must compatible with EMC, Vertitas, SAN or other renowned backup application. | ☐ Not Applicable<br>☑ Comply<br>☐ Not Comply | | |

☐ Not Applicable

☐ Not Applicable

| | | | | |
|---|---|---|---|---|
| 5. | The system has the backup/restore capability for a. Full systems backup such (application, production data, configuration, parameters and definitions etc) into removable media for offsite storage.<br>b. Backup files can be restored for business continuity.<br>c. Backed-up files recoverable instantaneously whenever required for forensic / investigation purposes | ☑ Comply<br>☐ Not Comply<br>☐ Not Applicable | | |
| 6. | The vendor is to provide a documented steps & procedures for the backup and restore process. | ☑ Comply<br>☐ Not Comply | | |
| 7. | Vendors sign individual NDA's to preserve the confidentiality of any proprietary information made available to them by Securitysense. | ☑ Comply<br>☐ Not Comply | | |

| **Compliances** | |
|---|---|
| Total No of Compliance (Comply) | **7** |
| Total No of Not Compliance (Not Comply) | **0** |
| Total No of Not Applicable (Not Applicable) | **0** |
| **Percentage Compliance:** ((Total Number of "Comply + Not Applicable" / 15) x 100%) | **100.00%** |

*__Note__: Please fill up the No. of **Comply/Not Comply and Not Applicable** fields then right click on the **percentage of compliance** field and click update, the % will be calculated automatically.

## Section F : SecurityRatings

| Total Number of Controls | # of Complied Controls | # of Not Complied Controls | # of Not Applicable Controls |
|---|---|---|---|
| **97** | **80** | **1** | **16** |

*__Note__: Please right click on # fields and click update, the # will be calculated automatically.

| **Ratings** | | |
|---|---|---|
| Section B: | General Controls | 92.86% |
| Section C: | Network Security Controls | 100.00% |
| Section D: | Application Security Controls | 100.00% |
| Section E: | Database Security Controls | 100.00% |
| Section F: | System Security Controls | 100.00% |
| Section G: | ID Security (OS, Application & Database) Controls | 100.00% |
| Section H: | Operation Security Controls | 100.00% |
| **Average Ratings** | | **98.98%** |

*__Note__: Please right click on the fields and click update, the % will be calculated automatically

**Assessor Particulars:**

**Name:** ????

**Designation:** ????

**Department/Division:** ????

**Company Name:** ????

**E-Mail:** ????

**Phone No:** ????

(Signature and Date)

**Declaration:**

We hereby declare that we have read and understood all the controls and ensure all complied controls will be implemented within project. Risk identification, assessment with Mitigation plan submitted with this document.

(Signature of PM & date) (Signature of Vendor& date)

| **Network Security and Audit Review/Comments:** |
| --- |
| |

Review/Comments By: (Signature and Date)

## Section G : Comments after Implementation

| **Vendor/Project Manager Review/Comments:** |
| --- |
| |

Review/Comments By: (Signature and Date)

| **Central Operations Review/Comments:** |
| --- |
| |

Review/Comments By: (Signature and Date)

| **Network Security and Audit Review/Comments:** |
| --- |

| |
|---|
| |

Review/Comments By: _____

(Signature and Date) _____

| **Approval from Head of Central Operations/User Division** |
|---|
| |

Approved By: _____

(Signature and Date) _____