SOC Sheet:

**Security criteria:**

**CC1: Organization and management**

**CC1.1: organization structure, reporting lines, authorities, and responsibilities are defined**

Control Activities:

1. Roles and responsibilities are mentioned in job description (job description)
2. Documented position description defines skills (job description)
3. Criteria is evaluated as a part of business planning process and updated with change in sys requirements (org chart, background chart)

**CC1.2: responsibility and accountability of work and risk mitigation strategies are properly assigned to to individuals by authorities**

Control Activities:

1. Candidates ability to meet requirements in job description are evaluated (job description)
2. Documented position description defines skills (job description)
3. work is allocated by leads only (jira work allocation)

**CC1.3: procedures are established to evaluate the competency of the person doing the work and resources are provided**

Control Activities:

1. Candidates ability to meet requirements in job description are evaluated (job description)
2. Documented position description defines skills (job description)
3. Employees are evaluated based on their knowledge of the skills (employee evaluation)
4. Resource manual is provided (resource manual)

**CC1.4: there is workforce conduct standards, background screening procedures and conducts enforcement procedure**

Control Activities:

1. Background checks are performed (background check policy)
2. Employee to accept code of conduct (code of conduct)
3. Employee verified against regulatory screening database (employee verification)

**CC2: Communications**

**CC2.1: info regarding design and implementation is communicated well to internal and external users to make sur they know their roles**

Control activities:

1. System description is available to external user on the customer facing website (external users)
2. System description is posted on company’s intranet for internal users. This description describes the boundaries of the system (internal users)

**CC2.2: company commitments are communicated to external users and also to internal users to carry out their work**

Control Activities:

1. Policies and procedures are available on intranet for internal users and internet for external users (policy mentioned on web)
2. Employee required to attend annual training (employee training)
3. Background checks performed
4. Sys requirements mentioned on internal portal (sys commitments for internal users)

**CC2.3: responsibilities of external and internal users are communicated to them**

Control activities:

1. System description is available to external user on the customer facing website (external users)
2. Employees are required to sign non disclosure (sensitive data security)
3. Employee required to attend annual training (employee training)

**CC2.4: information necessary for work is provided to personnel**

Control activities:

1. Policies and procedures are available on intranet for internal users and internet for external users (policy mentioned on web)
2. New hires and users requesting access are asked to sign a non disclosure (sensitive data security)
3. Training course are available (employee training)

**CC2.5: internal and external users have informatio on how to report failures, incidents and concerns**

Control Activities:

1. Internal users are updated with documentation on failures
2. SLA with users (SLA)
3. Customers can contact help desk anytime (customer care)

**(finding)**

**CC2.6: sys changes that results in change in responsibilities of users is communicated well to them**

Control Activities:

1. Segregation of duties
2. Training provided to internal users (employee training)
3. Documented position description defines skills (job description)

**CC3: Risk management and design and implementation of controls**

**CC3.1: company identifies potential threats(including vendors and third parties), analyzes the significance of risks, determines mitigation strategies, identifies changes and reassess the processes**

Control Activities:

1. Procedure in place for third party risk (third party risk)
2. Documented risk assessment process (risk assessment )
3. Understanding within employees of policies related to environmental and technological changes (tech change)

**CC3.2: company understands the risk mitigation processes and updates the control activities and operations based on that**

Control Activities:

1. Change control and quality management are in place to ensure changes are understood by all (change control doc)
2. Training is provided in case of change in roles and responsibilities (role training)
3. Internal vulnerability assessment is done regularly (vulnerability scans)

**CC4: Monitoring Controls**

**CC4.1: design and effectiveness of system are timely evaluated and necessary changes are made to the system**

Control Activities:

1. Documented escalation procedures are in place (escalation procedures)
2. Procedures are tested and errors are followed up (testing job)
3. The system is altered based on shortcomings (maintenance log)

**CC5: Logical and Physical access control**

**CC5.1: identification and authentication, restriction of authorized users, prevention and detection of unauthorized users**

Control Activities:

1. Documentation for installation and maintenance for users (operations and management manual)
2. Proper authentication on login (sqldbuser)
3. Segregation of duties
4. Passwords are maintained (passwords)

**CC5.2: new external and internal users are authorized before giving access to the system**

Control Activities:

1. New user access request are documented (event log config)
2. There is quarterly check of users who have been inactive (inactive users jira)
3. Logs of users added and removed is maintained (event log config)

**CC5.3: internal and external users are authenticated**

Control Activities:

1. Proper authentication on login (sqldbuser)
2. Passwords are maintained (passwords)
3. Double verification of user (2 step verification)

**CC5.4: access to data or software is authorized and modified based on roles**

Control Activities:

1. Pre defined security groups in database (roles group)
2. Removal of role is possible on database (removing roles)
3. Sys design change can change responsibilities of roles (sqldb user access)

**CC5.5: facility locations like datacenter, media storage and all are restricted to authorized personnel only**

Control Activities:

1. Data centers should not allow physical access to data (data center rules and regulations)
2. Proper id card is required to enter the location (data center rules and regulations)
3. Employees have signed contract saying no personal work of info at these locations and cannot use anything for personal work (policy for employee personal business)

**CC5.6: Logical access security measures are implemented**

Control Activities:

1. Web servers utilize TLS encryption (tls)
2. User authentication (login)
3. Passwords are maintained (passwords)
4. Double verification (2 step verification)
5. Different authority levels ()

**CC5.7: transmission, removal of information is restricted to authorized person only**

Control Activities:

1. Web servers utilize TLS encryption (tls)
2. VPN, SSL and SFTP(safe file transfer) is used (sftp, ssh)
3. DLP software is used to scan sensitive info (DLP software, data protection dashboard )
4. Info like ssn is blocked (data masking, data protection dashboard)

**CC5.8: Controls have been implemented in case of unauthorized access to system**

Control Activities:

1. Security monitoring application is implemented and email notification is send on virus or malicious activity (security monitor)
2. The ability to install software is done only by IT support (It support manual)

**CC6: System Operations**

**CC6.1: Vulnerabilities to sys breaches, or due to malicious acts or natural disasters or errors are identified, monitored and rectified**

Control Activities:

1. Vulnerability scans on the system are performed on regular basis (vulnerability scan)
2. Weekly full-system and daily backups are performed using an automated system. (backup schedule)
3. Data backup is monitored (data backup monitoring tool)
4. Data is securely being transferred to a safe link in case of disaster (data transfer securely)

**CC6.2: logical and physical security breaches are identified and reported to responsible personnel and acted on**

Control Activities:

1. Personnel follows a defined protocol to identify breaches. Security events are assigned to security personnel and privacy events to privacy personnel (Incident response policy)

(**SOD finding**)

1. Management meetings are held on weekly basis to identify events (meeting calendar)
2. Cyber attack procedure

**CC7: change management**

**CC7.1: commitments and system requirements are addressed during SDLC.**

Control activities:

1. System change requests are evaluated (monitoring tool)
2. Code changes and OS patches are tested (test patches, upgrade management)

**CC7.2: Data, S/W, policies and procedures are updated consistently to meet requirements**

Control Activities:

1. All of the above are evaluated for needed changes and a change req can be created (jira change management, change req creation)
2. Root cause analysis is done and change req is initiated (root cause analysis pdf, change req creation)
3. Management meetings are kept every week (meeting calendar)

**CC7.3: change management req is created when a deficiency in system or operations is noted**

Control Activities:

1. Root cause analysis
2. Incidents required to change follow standard change control process (change control process)
3. Change req is authorized before going ahead (change req authorization form)

**CC7.4: changes to system are authorized, designed, developed, configured, documented and tested**

Control Activities:

1. Sys changes must be approved before starting work. Separate personnel’s responsible for approval and work (change req authorization form)

**(SOD finding)**

1. Test data and plans are created. These are authorized before starting by a different personnel (test plan)
2. Regression testing is done and submitted to the developer (test recorder)
3. A monitoring tool is in place to administer all the changes going on (monitoring tool)

**Availability criteria:**

**A1.1: current capacity is maintained and the system is notified in case of additional capacity with increasing demands**

Control Activities:

1. Monitoring tool for in scope and alert personnel in case of threshold is met (alert policy)
2. Notified if additional capacity is required for new logins (alert login)
3. Monitoring tool is utilized to check if sys requirements are met (resource monitor)

**A1.2: environmental protections, data backup, recovery are authorized, designed, developed and maintained**

Control Activities:

1. Disaster recovery plans and procedures are in place (disaster recovery plan guide)
2. Data back up plan is developed and implemented (disaster recovery plan guide)
3. Accurate recovery time is estimated in case of disaster (recovery time)

**A1.3: disaster recovery plans are tested**

Control Activities:

1. Perform restoration testing of database back up files per release cycle.
2. Personnel needs to identify specific actions that will eliminate or mitigate consequences associated with specific problems in recovery.
3. the testing method should make sure that the organization can restore data, recover business applications and continue operations

(**Finding: There is a disaster recovery plan in place but it is not tested**)

**Confidentiality Criteria:**

**C1.1: confidential information is protected during design, development, implementation to meet confidential commitments**

Control Activities:

1. Client data is not used for testing (masking and agreement)
2. Test data is created that masks the client data (masking)
3. Data owners approved storage used for production (data ownership agreement)

**C1.2: Confidential data(in boundaries) is protected against unauthorized access, and use**

Control Activities:

1. Users are authenticated while login and minimum password requirement (login, passwords)
2. Creation and management of access controls for databases is through access provisioning process (access control)
3. Awareness training is provided to employees for usage of personal information (employee awareness pdf)

**C1.3: Confidential data (outside of boundaries) is restricted to authorized parties**

Control Activities:

1. Use of removable media is done only after authorization (deny write access, removable media policy)
2. Admin access in system are authorized (login)
3. A non-disclosure or confidentiality agreement is signed by all (data confidentiality agreement)

**C1.4: commitments are obtained from vendors and third parties**

Control Activities:

1. Agreements with third parties
2. User must sign third party policies too  
   **finding: There’s not enough guidance on managing contracts and risks related to the use of third parties**
3. A non-disclosure or confidentiality agreement is signed by all (data confidentiality agreement)

**C1.5: compliance with entity’s confidentiality with vendor, user and third parties are assessed periodically**

Control Activities:

1. Management reviews third party agreements annually (confidentiality agreement)
2. Site visits are performed on vendor management guidelines (site visit report)

**C1.6: changes to confidentiality commitment are communicated to users, vendors and third parties**

Control Activities:

1. Contracts are updated on change in confidentiality practice (changes to agreement)
2. Site visits are performed on vendor management guidelines (site visit report)
3. Vendor systems are reviewed and SOC reports are generated (vendor risk assessment)

**C1.7: entity retains confidential information**

Control Activities:

1. Documentation is in place regarding retention and disposal of confidential info (employee awareness)
2. Automated process for deleting of some information (scheduled deletion)
3. Info that is no longer required is regularly removed from the system (auto deletion)

**C1.8:entity disposes confidential information**

Control Activities:

1. Documentation is in place regarding retention and disposal of confidential info (employee awareness)
2. Automated process for deleting of some information (scheduled deletion)
3. Info that is no longer required is regularly removed from the system (auto deletion)