Auditoria.AI SmartFlow Skills Application and Data Security Checklist

Digital Transformation has become a critical business imperative for companies, regardless of industry vertical, size, and operating scale. The acceleration of digital transformation has led to greater adoption of cloud computing and Software-as-a-Service (SaaS).

Security requirements such as Assessments, Monitoring, and Visibility have become fundamental prerequisites to these transformational projects. With new technologies like Artificial Intelligence (AI), Machine Learning, and Automation, there is a rise in the target attack surface.

Security in the cloud has been one of the biggest concerns that has prevented organizations from adopting cloud-based ERP applications en masse. However, in recent years there has been a marked improvement in cloud security.

This document presents critical security considerations when extending ERP and accounting applications with AI and Automation. It is intended to be a best-in-class security and privacy checklist assessment to use when evaluating ERP-centric AI and Cognitive Automation investments.

Application & Interface Security

1. Automated source code analysis detects security code defects before production.
2. Review applications for security vulnerabilities and address any issues prior to deployment to production.
3. All identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting access to data, assets, and information systems.

Audit Assurance & Compliance

4. Allow tenants to view third-party audit or certification reports (SOC2/ ISO 27001).
5. Network penetration tests of cloud service infrastructure annually.
6. Conduct application penetration tests of cloud infrastructure regularly as prescribed by industry best practices and guidance.
7. Monitor changes to regulatory requirements in relevant jurisdictions, adjust security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements.

Business Continuity Management & Operational Resilience

8. Business continuity plans tested at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.
9. Policies and procedures established and made available for all personnel to adequately support services operations' roles.
10. Technical capabilities to enforce tenant data retention policies.
11. Implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements.
12. Test backup or redundancy mechanisms at least annually.

Change Control & Configuration Management

13. Restrict and monitor the installation of unauthorized software onto systems.

Data Security & Information Lifecycle Management

14. Provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet).
15. Utilize open encryption methodologies any time infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another).
16. Procedures in place to ensure production data shall not be replicated or used in non-production environments.
17. Support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data.

Datacenter Security

18. Maintain a complete inventory of all of critical assets located at all sites/ or geographical locations and their assigned ownership.
19. Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems.
20. Restrict physical access to information assets and functions by users and support personnel.

Encryption & Key Management

21. Encrypt tenant data at rest (on disk/storage) within environment.

Governance & Risk Management

22. Documented information security baselines for every component of infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.).
23. Formal disciplinary or sanction policy established for employees who have violated security policies and procedures.
24. Notify tenants about material changes to infosec and privacy policies.
25. Perform annual reviews to privacy and security policies.

Human Resources

26. Upon termination of contract or business relationship, employees and business partners adequately informed of their obligations for returning organizationally-owned assets.
27. Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and involved third parties subject to background verification.
28. Employment agreements incorporate provisions/terms in adherence to established information governance and security policies.
29. Annual personnel training and awareness programs.

Identity & Access Management

30. Restrict, log, and monitor access to information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.).
31. Monitor and log privileged access (e.g., administrator level) to information security management systems.
32. Controls in place ensuring timely removal of systems access that is no longer required for business purposes.
33. Manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access.
34. Controls in place to prevent unauthorized access to application, program, or object source code, and assure it is restricted to authorized personnel only.
35. Controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only.
36. Document how grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege.
37. Require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by tenants), based on the rule of least privilege, by business leadership or other accountable business role or function.
38. Timely deprovisioning, revocation, or modification of user access to systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties.

Infrastructure & Virtualization Security

39. File integrity (host) and network intrusion detection (IDS) to facilitate detection, investigation by root cause analysis, and response to incidents.
40. Physical and logical user access to audit logs restricted to authorized personnel.
41. Audit logs reviewed on a regular basis for security events.
42. Operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls as part of baseline build standard or template.
43. Logically and physically segregate production and non-production environments.
44. System and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements.
45. Restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles).

Security Incident Management, E-Discovery, Cloud Forensics

46. Documented security incident response plan.
47. Tested security incident response plans in the last year.
48. Predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.

Supply Chain Management, Transparency, & Accountability

49. Security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).
50. Third-party agreements include provision for the security and protection of information and assets.
51. Capability to recover data for a specific customer in the case of a failure or data loss.
52. Tenants provided with ongoing visibility and reporting of operational Service Level Agreement (SLA) performance.
53. Mandate annual information security reviews and audits of third party providers to ensure that all agreed upon security requirements are met.

Threat & Vulnerability Management

54. Anti-malware programs that support or connect to cloud service offerings installed on all of IT infrastructure network and systems components.
55. Capability to patch vulnerabilities across all of computing devices, applications, and systems.

About Auditoria

Auditoria is an AI-driven SaaS automation company for corporate finance that automates back-office business processes like tasks, analytics, and responses.

By leveraging natural language processing, artificial intelligence, and machine learning, Auditoria's platform removes friction and repetition from mundane tasks while also automating complex functions, such as predictive analytics.

Corporate finance and accounting teams use Auditoria to accelerate business value while minimizing heavy IT involvement, improve business resilience, lower attrition, and perform higher-level business functions. Give your finance teams superpowers at Auditoria.ai.