MIS 5202
12/10/15
IT Governance
Audit Plan Project
Yizhou An, Jiehong Huang, Blake Koen,
Anh Tran and Shizhong Yang

Audit Plan For ABC Company's Social Security Number Policy

I. Background

During the course of daily business, ABC Company will collect Social Security Numbers (SSNs) and other Personal Identifying Information (PII) for such activities as establishing accounts and completing our day to day operations. As a result ABC must ensure that they have taken proper safeguards to ensure that our customers' SSNs are not left open to vulnerabilities that can lead to data breaches. A breach can be disastrous to the customers of ABC and the company itself. Reasons for this include:

- Customers identity and financial well being will be at risk.
- Company's reputation will be at risk.
- Financial loss due to legal settlements and credit monitoring services.
- Regulatory fines and penalties.

ABC has recognized the need for strict guidelines regarding SSNs and will be reviewing its current SSN policy to ensure that that the policy that is in place is adequate in protecting their customers against any potential leaks of personal information. The policy will be reviewed now and every 12 months thereafter.

II. Objective

The objective of this audit is to provide an assessment of the effectiveness and design of the SSNs policy. Also, authenticate that controls are in place to ensure compliance with regulation and standard and sensitive customer data and information are confidential.

III. Scope

ABC corporation collects and maintains personal information including SSNs. The scope of this audit report is limited to SSNs Policy; including but not limited to controls in place for SSNs Usage, Guidelines and Safeguards.

IV. Out of scope

This audit will not review controls related to Access Control, Personnel Control and Physical

Security Control. Those three controls will be assessed in their own audit policy.

VI. Control testing and Evidence

Control Objective	Current Controls	Control Testing	Evidence
Approved uses of SSNs	Only The last 4 digits of the SSNs can be used for account verification.	❖ Interview and observe employees that do have to verify accounts. ❖ Review any forms that contain SSNs.	❖ Review access log and evidence of SSN usage.
Policy Reviews and Regulation Compliance. ABC must ensure that they are in compliance with state and federal laws when collecting, using and storing SSNs.	Legal department and IT review compliances policies yearly and will update the policy based on newly implemented regulations.	❖ We will verify that the policies are up to date by interviewing managers and employees that are in charge of compliance. ❖ The policy shall be reviewed when laws are changed to ensure that the policy was adjusted.	❖ Change/update log ❖ Recent regulation change ❖ Compliances policies
Technology Standards. Information Technology will ensure that software and hardware are up to date.	Review the configuration map and technology inventory.	❖ Logical access is reviewed and tested, employees should be monitored to ensure full system access configuration is adequate.	❖ Review software and hardware build requests and ensure checklists are completed for each deployment. ❖ Current configuration map ❖ Current technology inventory
Information Security will ensure that files containing SSNs are properly deleted.	Retain audit logs when deleting SSNs data. Use secure data	❖ Review the audit logs. ❖ Ensure that the data deletion tools	❖ Current copy of audit logs ❖ Instruction of secure data deletion tools, if the service is outsourced,

	deletion tools to delete confidential data, instead of dragging files to the recycle bin.	are working properly.	review the SLA ❖ Current data retention policy
Proper Disposal of physical assets containing SSNs	Information Security shall ensure that paper and computers, disks, and other hardware that contain SSNs are destroyed in a secure manner.	❖ Interview employees in charge of destruction. ❖ Observe destruction. ❖ Review documentation related to disposal of physical assets containing SSNs	❖ Documentations related history of physical destruction ❖ Policy and procedures on physical destruction
Safeguarding SSNs	Data Security. All data is encrypted and stored behind a firewall.	❖ Penetration testing on data containing SSNs. ❖ Review logical access of data. ❖ Security audit logs are reviewed daily.	❖ Review data classification and firewall configuration. ❖ Review process for security monitoring.
Mail and Email controls.	Email and mail controls. SSNs are not permitted to appear in Emails or mail.	❖ We will randomly interview employees about SSN and outgoing mail and emails. ❖ Monitoring to ensure that there is no SSN included in any emails. If have to include a SSN in an email, make sure the email is under proper use and is secure.	❖ Review email and mail documentation.
Policy Violations	Deterrent control to prevent violations of the SSNs Policy	❖ Randomly interview employees about the violations	❖ Employee disciplinary reports ❖ Social Security Policy ❖ Social Security Policy

		procedures. Interview managers about violations.	violations log
Human resources will review the manual.	Ensure sufficiency of the employee manual	❖ Employee training program should be tested to ensure the policy is used and is understandable.	❖ Review employee interviewing report.

VII. Document request

SSN Policy
SSN Training manual
Access Control Policy
Physical Security Policy
Personnel Policy
Change Management Policy
SSN File Audit Logs
Data Retention Policy