COBIT 5 Based Audit Plan for CRM Systems

Julia Onchieku  
Department of Information System and assurance Management  
Concordia University of Edmonton.  
Edmonton, Canada.  
jonchiek@student.concordia.ab.ca

Sergey Butakov, Shaun Aghili  
Department of Information System and assurance Management  
Concordia University of Edmonton.  
Edmonton, Canada.  
{shaun.aghili, sergey.butakov}@concordia.ab.ca

Abstract—The research paper analyzes audit tests, steps and metrics for customer relationship management (CRM) systems. The features and risks associated with CRM systems have been discussed in depth to provide ground for the auditing approach. The research resulted in an audit plan that is specific to CRM systems. The audit plan was partially tested on open source SugarCRM. Results of the tests indicated that the features of CRM systems need specific controls to be put in place to protect the systems from the risks identified.

Keywords—CRM systems; audit plan; controls; security posture.

I. INTRODUCTION

The last two decades have seen the upsurge of computational capability that has led to exponentially increasing data flow. This increase has called for better forms of data processing and customer relationship analysis tools [1]. Customer Relationship Management (CRM) system is an example of such tools that are commonly used in nearly all sectors of industry. CRM involves the use of technology to integrate customer interactions with the business through data analysis [2].

Companies analyze customers’ data using CRM systems to help with making important decisions. The analysis provides a clear view of the client base and helps managers to decide how cross-selling of products can be done and which clients the organization should focus more attention on [3]. With the Big Data technologies adding momentum to analytical capabilities, CRM utilization will continue to grow.

A. Risks associated with CRM systems

Despite the various benefits of CRM systems, they come with some business risks. The main risks associated with the systems are: (1) Occurrence of system downtime or service unavailability [4]; (2) Insufficient, poor quality, and incorrect data in databases leading to wrong decision-making by the managers relying on the data [5]; (3) Unsuccessful data conversion may strain a CRM system and cause technical difficulties and, in the long run, significant financial costs [5]; (4) Data breaches and malware attacks may occur leading to loss or theft of critical data e.g. personal information of clients like credit card numbers. As a result of the occurrence of the data loss instances and theft of critical data, customers may leave the organization leading to loss of reputation and decrease in profits[6].

Some well-known large scale data breaches in CRM systems include break-ins into CRM systems at JP MorganChase, Salesforce and TalkTalk. In 2014 JP MorganChase bank data breach on their CRM systems lead to the compromise of personal information of millions of households and small businesses [6]. Data breaches happen in various components of IT including CRM systems. For example, the major data breach from JP Morgan Chase’s CRM, which compromised the private information of 7 million small businesses and 76 million households in 2014. The attack affected the bank’s reputation, finances and intellectual property in the form of marketing secrets [6].

Data breach cases like the ones above, provide a call to improve the security posture of CRM systems to prevent such events from happening. One of the avenues for the improvement in this area would be to establish consistent procedures for auditing of CRM systems. Use of audit plans specific to CRM systems can reduce the chances of having lower quality, nonspecific and inconsistent results comparing to the use of general IS auditing programs.

To solve the problem of potential inconsistencies and oversights in audit results of CRM systems, an audit plan has been developed as part of this research. The audit plan will benefit auditors looking for an effective program that is specific to CRM systems but provides enough flexibility to adjust it to a particular CRM implementation. The risks specific to CRM systems have been outlined, and COBIT 5 for Risk and COBIT 5 Risk Scenarios documents have been used to perform the risk analysis. The results of the risk analysis helped to identify the audit areas that are specific to CRM. Specific metrics for the audit will be outlined, to help check whether the goals for the different aspects of information security for CRM systems have been achieved. Controls have been checked and tested on a sample CRM system (SugarCRM).

II. EXISTING AUDIT CONSIDERATIONS AND RELATED WORK

A. Security in CRM

Examples of well-known CRM systems vendors include Salesforce, SAP, Siebel, Microsoft Dynamics and SugarCRM. IS audit aims at ensuring the effectiveness and efficiency of management processes to ensure service delivery. Some of the auditors’ responsibilities are development and implementation of an Information Security Audit strategy that is in compliance with the industry standards. Auditing helps the IS auditors to give assurance that the organization’s systems are controlled, assessed and monitored for the best performance [7].

B. Related standards and existing audit programs

Different organizations have both national and international interactions with stakeholders (partners, customers, vendors and shareholders). The international business practices brought up the need for industry frameworks and standards to secure information and data exchange processes [8]. Examples of useful documents for the development of information systems audit plans include (1) COBIT 5 framework and related documents (used for governance and management of IT) (2) ISO 27000 family of standards (for information security systems policies, standards and, procedures) and (3) NIST 800-53 (a framework for security and privacy controls made for IS in the federal organizations in the USA). Use of industry frameworks brings required level of credibility to the programs as these
In 2009, ISACA developed a Generic Application Audit and Assurance program [9]. The program was designed to be used by audit and assurance professionals to review various types of enterprise applications. That same year, Salesforce’s CRM Security Audit Guide was written for Salesforce CRM systems [10]. This research identified the differences between the Generic audit plan and the Salesforce audit plan with the goal of showing some gaps that were addressed in this research. Although the two plans serve different purposes, looking at the common elements is helpful in understanding what the industry uses to audit CRM systems.

The Generic Applications plan was designed to perform comprehensive audit and assurance for all applications while the Salesforce program was designed to perform security audit for Salesforce CRM systems. Some audit areas are discussed on the Generic program and not discussed on the Salesforce program, resulting in a gap. Use of the vendor specific audit plan saves the auditors time spent in going through details that are not relevant to the CRM system and gives more credibility to the results of the audit. Use of the audit plan provides the IS auditors an efficient audit tool that will provide consistent results. However, being vendor specific, the Salesforce audit plan may not be appropriate to use on other types of CRM systems. There are other CRM specific audit programs on the market such as Microsoft Dynamics audit plan [11].

### TABLE 1: Sample of audit procedures and metrics that check for generic risks in CRM systems with reference to Generic applications audit/assurance plan by ISACA.

<table>
<thead>
<tr>
<th>RISKS</th>
<th>COBIT 5 FOR RISK SCENARIOS REF.</th>
<th>AUDIT PROCEDURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>Audit planning and scopeing for CRM systems</td>
</tr>
<tr>
<td>1.</td>
<td>Program not aligned to the corporate strategy</td>
<td>0101</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Failure of project through poor scoping.</td>
<td>0101 0201</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order to look into CRM-specific risks table 2 maps the features of CRM systems to the potential risk scenarios outlined in COBIT 5 for Risk document. There is a column with the reference codes in the risk scenarios. Table 2 provides audit procedures and applicable metrics that could be used to check for the risks in the features of CRM systems. For example, taking the first row of Table 2, the risk of data modification leads to insufficient, poor quality and incorrect data in the CRM data warehouse. This risk can affect data analysis and reporting leading to poor decision making. Data modification risk is found in the COBIT 5 for Risk under Ref. no. 0607 (Data
(accounting, security-related data, sales figures, etc.) are modified intentionally). An audit procedure that can be used to check for the risk is checking the login and authorization settings default setting

TABLE 2: Audit tests, steps, and metrics that check for risks associated with the features of CRM systems.

<table>
<thead>
<tr>
<th>FEATURES OF CRM SYSTEMS</th>
<th>RISKS</th>
<th>COBIT 5 RISK SCENARIOS</th>
<th>TESTING PROCEDURES</th>
<th>APPLICABLE METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data analysis and reporting</td>
<td>Insufficient, poor quality and incorrect data in the databases can lead to bad decision making by the managers relying on the data. Poor quality and inaccurate data in the data resources frustrates the users of the data and leads to incorrect marketing [5]. People with malicious intent can log into the system and manipulate data. <strong>Inability to access data</strong> - A faulty system can also make data inaccessible to the people who need it.</td>
<td>0607 0601 0501</td>
<td>Login and authorization settings - check the default setting of the CRM system and the restriction options that can be selected for more system security. Confirm that terminated or resigned employees do not have access to the system. Check the database management, data analysis and reporting processes - Is the data resulting from the analysis done by the CRM system correct and of good quality according to the records?</td>
<td>Password timers, Password history, Password complexity, Number of invalid password attempts that lead to lock out, Data quality, high, medium or low.</td>
</tr>
<tr>
<td>Process automation - CRM systems do automation of business processes related to customer care, which reduces money and time spent on data entry.</td>
<td>The potential loss of data - If the CRM system becomes faulty and messes up process automation some data might get lost. <strong>Inability to access data</strong> - A faulty system can also make data inaccessible to the people who need it. <strong>Customer dissatisfaction</strong> - Using process automation for customer service call systems, may lead to frustrated customers when calls are not being picked up by live operators. <strong>Decrease in innovation of employees</strong> as a result of machines doing most work [12]</td>
<td>0909 0901</td>
<td>Check the CRM systems automation processes - Are there cases of data loss, system inaccessibility, and customer dissatisfaction due to failure in the systems' automated processes?</td>
<td>Number of cases of failure of processes</td>
</tr>
<tr>
<td>Integrating with other applications The integration helps the organization to maintain relevant, accurate information about customers.</td>
<td>Data modification - Non-integration of CRM systems with other business applications like ERP systems compels the use of manual processes e.g. manual data entry that may allow intentional or unintentional errors leading to data modification. <strong>Manual data entry errors</strong> may also lead to incorrect marketing that may cause the organization financial losses. <strong>Software system issues</strong> - If one of the applications being integrated with the CRM is compromised with malware, the integration may pose the risk of infection to the CRM system. <strong>An increase in the risk of fraud</strong> - Through use of manual processes, [4].</td>
<td>0503 0504</td>
<td>Find out whether permission to access the CRM systems is only granted to the people who use the systems and that unauthorized individuals do not gain access. Are the systems only accessed by authorized individuals? Are there cases of unauthorized individuals accessing or trying to access the system e.g. hackers? Are there cases of malicious interruption or denial of services?</td>
<td>Number of unauthorized system access cases</td>
</tr>
</tbody>
</table>
To save the space, full names and narratives for each of the scenarios from COBIT 5 for Risk document are not placed in the table 2 but can be found in COBIT 5 for Risk in section 2B, chapter III. Specific features outlined in table 2 outlines directions for risk mitigation in CRM systems.

C. Audit Steps, tests, and Metrics for CRM systems

The risks associated with CRM systems identified in Table 2 require controls to be put in place. The controls are put in effect to mitigate risks. Auditing requires steps, tests and metrics which, in this research, were developed considering the Salesforce security audit plan and the generic applications audit/assurance plans. To start with, Table 1 above shows the audit tests to be taken to check for generic risks in CRM systems. It maps the tests to the potential risk scenarios outlined in COBIT 5 for Risk document. Most of the risks identified in Table 2 are not in Table 1 because Table 2 is addressing risks that are specific to the features in CRM systems. This paper will not provide a detailed discussion of the risks in table 1 since the risks are generic in nature.

The risks identified in Table 2 have been linked to the audit procedures and metrics that can be used when auditing. For example, take the first risk of occurrence of system downtime or denial of service attack which is found in the COBIT 5 for Risk document, Ref. no. 1601. The risk can be identified by checking the login and authorization and password settings. One of the metrics for this test is password timers. The narrative of Ref. no. 1601 is ‘Unauthorized users try to break into systems.’ The complete discussion of Table 2 is not provided here due to the limitation of space.

The audit procedures in Table 2 represent a plan based on COBIT 5 framework and Salesforce CRM security audit plan that will help IS auditors to audit CRM systems to improve the security posture of the business they are auditing.

D. Performance evaluation of the security features in SugarCRM system

The proposed audit plan in Table 2 was used here to perform an evaluation of the security features and controls in SugarCRM system. The evaluation template could be used by auditors or security analysts to check whether the CRM system they want to purchase is good for the organization where the system will be implemented. Use of the template will ensure the CRM system being acquired will uphold a high level of information security. The auditor/system analyst will identify the risks they want to check controls for then use the audit tests mapped to the risk to do product evaluation. Below is an evaluation template that can be used to review data breach risk for security before implementing a CRM system. The audit tests are found in detail in Table4 above.

E. Audit Tests and results

1. Password settings- Passwords are set up for different users. The settings have the option to enable password expiration as a security control. However, there are no minimum security requirements for the passwords. The absence of minimum security requirement means a user may set up a weak password which can be hacked to access the system.

2. Session settings- Settings are enabled to restrict active user sessions. If a user leaves the system active and moves away for a certain period, they will be logged out. This prevents unauthorized users from having access to the systems.

3. Login and authorization settings- When login into the SugarCRM system, a specific URL is used to establish login settings, providing a security mechanism.

4. Data privacy settings- Different users of SugarCRM can be allocated access permissions and different roles according to profiles.

5. System audit features- The systems has audit features, however not by default. The user of the system has to select the fields they want an audit trail from and select the audit function. The audit function helps to trace the source of a security breach if any.

6. Database management, data analysis, and reporting processes- SugarCRM uses common database functionality and supports different database systems like MySQL. Due to this database errors may occur if the database system isn’t working well with SugarCRM. The reports function in the system can provide a powerful data analysis and reporting tool.

7. Systems automation processes- The system has automation processes e.g. for sales and marketing, but some data has to be manually input and may bring some data breach issues.

8. Access control settings- Different access privileges are granted to different user profiles. The settings deny access to unauthorized individuals who may want to perform a data breach.

9. Ability to integrate with other applications to maintain relevant and accurate information- SugarCRM can be integrated with other applications e.g. the email system, ERP, and social websites.

10. Organization’s network management and website Integration- The network settings can be configured to be secure to allow for safe website integration e.g. when collecting sales leads from websites.

11. Scalability of the system- SugarCRM allows the effective addition of apps.

12. Data migration is done properly- With SugarCRM data migration is done between on-site and on-demand environment. There are different requirements for successful data migration.

13. Customer support- Customers have the ability to report cases and ask questions. They can also get access to different helpful articles. The different customer cases can be assigned to different employees to be solved. SugarCRM also does call center management.

The features and controls of SugarCRM were checked as above. For example, when password settings were checked, it was found that there are no minimum requirements for password complexity in the SugarCRM that was tested. Security can be tightened in the system by setting minimum requirements for secure passwords. E.g. Capitalization of some letters in the password and mixing of characters. Auditing of the system checks for the presence of security controls that protect data. After the audit, auditors can give
recommendations on the measures the organization can take to improve the security controls.

IV. CONCLUSION & RECOMMENDATIONS

This paper attempted to answer the research questions related to the specific features of CRM systems and risks associated with these features. Subsequently, the research looked into the controls and metrics related to the risks and the audit procedures that can be performed to check for the existence, effectiveness and efficiency of the controls. Metrics for CRM systems were developed based on the risks, audit steps and tests of this research. An audit plan was developed to help companies identify which areas they should concentrate on in an attempt to improve CRM systems security effectiveness and efficiency. An auditor using the audit plan will be able to give assurance that the systems have controls in place to protect the company’s information assets and hence profits.

This research provides IS Audit professionals a CRM specific plan to use for CRM systems from different vendors. The research has contributed to the audit considerations and risk analysis. Use of the CRM specific audit plan on CRM systems will further increase the level of security. The audit plan provided step by step audit procedures that can be used by different types of organizations. However, the IS auditors may have to adjust and customize the plan according to the specific needs and circumstances of an organization. Potential directions for the future research in this area may include a research on a security-focused product evaluation template for database management systems based on a well-known industry framework.

REFERENCES


