Information System Analysis

of LafargeHolcim

SAP

April 22, 2018

Institute of Information Technology
University of Dhaka

Submitted To

Mr. Md. Iftekharul Amin
Assistant Professor
Institute of Business Administration
University Of Dhaka

Submitted by

Group 5
Mahir Mahbub 0807
Atiq Ahammed 0817
Khayrul Islam 0822
Sefat-E-Mahadi 0839

BSSE 08th batch

Institute of Information Technology

University of Dhaka

Letter of Transmittal

Mr. Md. Iftekharul Amin

Assistant Professor

Institute of Business Administration

University Of Dhaka

Subject: Submission of final report on Information System Analysis of LafargeHolcim.

Dear Sir,

With due respect, we are pleased to submit the final report on Information System Analysis of LafargeHolcim. Although this report may have shortcomings we did try our level best to produce an acceptable report. We would be highly obliged if you overlooked our mistakes and accepted our effort we put in this report.

Sincerely yours,

Mahir Mahbub 0807 _____

Atiq Ahammed 0817 _____

Khayrul Islam 0822 _____

Sifat-E-Mahadi 0839 _____

BSSE 8th batch

Institute of Information Technology

University of Dhaka

Acknowledgement

We are highly indebted for getting such a tremendous opportunity to prepare the report on Information system analysis of LafargeHolcim. We would like to thank whole-heartedly our course teacher, Mr. Md. Iftekharul Amin, Assistant Professor, Institute of Business Administration, University Of Dhaka, for giving us guidelines about how we can prepare this report. In completing this paper we have collected various important data and information from Md. Majharul Huda Lizan, Manager, logistics cost control LafargeHolcim Bangladesh Limited. We are thankful to all of the works cited.

Executive Summery

LafargeHolcim is a manufacturer of building materials (primarily cement, aggregates, and concrete), with a presence in around 80 countries and 81,000 employees being the largest in the world. It was formed by the merger on 10 July 2015 of cement companies Lafarge and Holcim, which had combined net sales of CHF 26 billion in2017. On 7 April 2014, Lafarge and Holcim announced a merger project to create LafargeHolcim. As a large organization, LafargeHolcim has to consume and maintain a huge amount of information about business procedures, business materials and also about all employees. Between those, all information some are very confidential and some are not so much. On the other hand, different employees or members of the organization has a different role on that information based on their access. This requires an information system to not only easily maintain that information but also to provide secure maintenance.

LafargeHolcim uses SAP information system, as they found it more secure, dynamic and easy to use for their employees and their all requirements are almost fulfilled by this information system.

Contents

Tables & Figures

Glossary of Terms and Abbreviations

ACS – Affiliated Computer Services, Inc. The vendor supporting the Department' information system.

Application-level Controls – controls incorporated directly into computer applications t ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.

COFRS – Colorado Financial Reporting System. The financial information system that maintains the official accounting records for Colorado state government.

CPPS – Colorado Personnel and Payroll System. State system that maintains data on employee demographics, employee salaries, and job classifications.

Computer Application or Application – a computer program or set of programs that perform the processing of records for a specific function. Examples of computer applications include Microsoft Office, Microsoft Excel, COFRS, and SAP.

Department – LafargeHolcim enterprise

Enterprise Resource Planning System – an information system designed to integrate and streamline an organization's business processes, including accounting, purchasing, human resources, and other functions.

Firewall – a router, server, or specialized hardware device designed to restrict access to one network from another network.

FMIS – Fiscal Management Information System. The Federal Highway Administration's system for managing federally funded highway projects within the Federal-aid Highway Program.

FTE - Full-time equivalent. An FTE of 1.0 means that the person is equivalent to a full-time worker, while an FTE of 0.5 signals that the worker is only half-time.

General Computer Controls – controls that relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to ensure the proper development and implementation of computer applications and the confidentiality, integrity, and availability of program and data files.

IDS – Intrusion Detection System. An automated system that inspects network activity to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

IP Address – Internet Protocol Address. A numerical label assigned to computers and devices participating in a network, such as the Internet.

IT – information technology.

IT Infrastructure – all information technology assets (hardware, software, data), co
systems, applications, and resources.

OIT – Governor's Office of Information Technology. The state agency within the Govern
that is responsible for the administration, management, and oversight of state IT operations and systems.

SAP – Systeme, Anwendungen, Produkte (German for Systems, Applications, and Products). The proprietary, integrated enterprise resource planning software developed and owned by SAP AG, a German software development and consulting corporation.

VPN – Virtual Private Network. A protected information system link utilizing tunneling, security controls, and end-point address translation providing the same function as a secured, dedicated line.

1 Introduction

LafargeHolcim's industrial operations have a wide geographical footprint and are usually present in a territory for an extended period of time. In addition, their cement, concrete, and aggregates activities are all local businesses, where manufacturing is often close to the selling point and final customer. Therefore, their operations have an impact on local communities and people's lives.

At LafargeHolcim, they believe this impact can be positive. They also think our solutions can provide answers to challenges affecting the communities where we operate, such as urbanization, housing needs, health & safety and human rights.

1.1 Background

LafargeHolcim is responsible for producing cement, concrete, maintaining and constructing the state-owned transportation system. Specifically, these responsibilities include operating the State's highway system, managing highway construction projects, and maintaining the statewide aviation system plan.

Based on evolving business needs and the costs associated with maintaining existing systems, Department management decided to procure and implement an enterprise resource planning system to consolidate its primary business functions-including accounting and budgeting, human resources, time entry and payroll, project management and reporting, highway maintenance, and procurement-into one modern, adaptable system. The Department selected SAP for this modernization initiative. The Department reports that the ongoing budget for the operation and development of SAP is approximately $9 million annually, including state personnel and contract staff, computer operations (software, power, security), and new capital purchases (i.e., hardware). Every division and workgroup within the Department uses and relies upon SAP to accomplish essential business functions. The system's almost 3,200 users are located throughout the state and depend on SAP to provide up-to-date and accurate information. Additionally, SAP interfaces or sends critical financial, payroll, and highway project data to state and federal systems and agencies, including to the Colorado Financial Reporting System (COFRS), Colorado Personnel and Payroll System (CPPS), and the Federal Highway Administration's Fiscal Management Information System (FMIS).

1.2 Origin

This report contains the results of an information technology audit of LafargeHolcim SAP information system. As we are the students of information technology, our goal is to be in introduced with this information system and briefly analyze it. Hence the report is originated to describe the SAP information system.

2 Objective

2.1 Board Objective

Analyze the overall information system of LafargeHolcim.

2.2 Specific Objective

This project is for studying the information system of LafargeHolcim. We found that they use SAP information for maintaining their full organization. Our main aim is to:

- Analyze the SAP information system
- Knowing how it works?
- How the members and employees of the organization interact with it?
- Why they think SAP can provide them better maintenance?
- What is their recommendation for SAP to serve more?

2.3 Scope

To meet the project objective we met with. Through this interview, we try to collect the information from him about the information system of LafargeHolcim. We also analyze some other document about SAP information system from SAP's web site and other organization's report on SAP.

2.4 Limitation

Although we have tried our best to accomplish the goal of this project on analyzing information system of LafargeHolcim, there were some limitations we had to face. These are-

- **Lack of time:** For the time limitation we could not gather more information to justify exact condition. The time constraints are limiting factors.
- **Questionnaire limitations:** As we were not initially introduced with any organization's information system, our questionnaire was a little bit limited.
- **Interview limitations:** Because of our limited time and scope, we were unable to take interview of an adequate number of employees of LafargeHolcim.
- **Lack of Knowledge and Experience:** As university level students, we lack in the knowledge of how an organization maintains its overall information. We also have limitations of experience of any organization whole information system.

3 SAP

SAP SE is one of the largest vendors of enterprise resource planning (ERP) software and related enterprise applications. The company's ERP system enables its customers to run their business processes, including accounting, sales, production, human resources and finance, in an integrated environment. The integration ensures that information flows from one SAP component to another without the need for redundant data entry and helps enforce financial, process and legal controls. It also facilitates the effective use of resources, including manpower, machines and production capacities.

According to its 2016 corporate fact sheet, SAP serves more than 335,000 customers in 190 countries, of which 80% are small- and-medium sized businesses (SMB). The latter fact is a more recent departure from the company's previous focus on large enterprise organizations. It's estimated that 75% of all global business transactions come in contact with an SAP system. The company offers on-premises, cloud and hybrid deployment models, with cloud computing options being the focus for the company's future. On the Forbes 2016 list of "The World's Biggest Public Companies," SAP was ranked the third-largest software and programming company, behind Microsoft (1) and Oracle (2) and is currently headquartered in Walldorf, Germany.

3.1 SAP Labs and Acquisitions

SAP says its primary focus on growth rests on internal innovation by developing and improving its own products. As a step in that direction, the company created SAP Labs, which are research and development locations that develop and improve core products. These are located in high-tech clusters around the world, such as in Bangalore, India, and Palo Alto, Calif.

Beyond organic growth, SAP has executed on an aggressive acquisition strategy to fill its technology gaps. Since 1996, the company has made more than 60 acquisitions. A major focus for the company in recent years has been building its cloud computing capabilities and enabling greater mobility. Acquiring companies with such technologies have helped to build those capabilities. Here are six acquisitions that serve as examples:

- Concur Technologies, 2014, online travel and expense management software as a service
- Fieldglass, 2014, cloud-based contingent labor and services
- Hybris, 2013, e-commerce, part of the SAP Customer Engagement and Commerce suite
- Ariba, 2012, cloud-based B2B marketplace
- SuccessFactors, 2011, cloud-based human capital management
- BusinessObjects, 2007, business intelligence.

3.2 SAP User Groups

An important part of SAP's information dissemination and engagement has been its user groups. These are independent, not-for-profit groups designed to help educate members, create customer involvement, give voices to users in influencing SAP strategy and provide networking opportunities. Here, SAP employees and users can meet and share information, experiences and lessons learned. Arguably more important, SAP hears user feedback in both the technical areas

and the functional areas. User groups are organized by region across the globe, with ASUG (Americas' SAP Users' Group), being the largest.

3.3 History of SAP

SAP was started in 1972 by five former IBM employees in Mannheim, Germany. The original name for SAP, Systeme, Anwendungen, Produkte, is German for "Systems, Applications and Products." The original idea for SAP was to provide customers with the ability to interact with a common corporate database for a comprehensive range of applications in real time.

In 1973, SAP released R/1, a financial accounting system. R/1 ran on IBM servers and DOS, and it had a single-tier architecture in which presentation, applications and data were on one platform.

In 1979, SAP released R/2, a mainframe system that provided real-time data processing across accounting, manufacturing, supply chain and human resources. R/2 used a two-tier architecture, where presentation was on one platform and applications and data were on another. R/2 helped power SAP's growth, and the vendor expanded its customer base to about 200 companies.

In 1992, SAP released R/3, which represented a switch from mainframe computing to the client-server model, and from a two-tier to a three-tier architecture, in which presentation, applications and data were housed separately. R/3 was a critical product for SAP that launched the company onto the world stage.

In 1999, SAP launched mySAP, which marked a new strategy for the company of focusing on combining e-commerce software with the applications in R/3. One year after R/3's release, SAP partnered with Microsoft to port the new version to Windows NT. By 1997, SAP employed 13,000 people.

In 2004, the company launched SAP NetWeaver, and it reported that more than 1,000 customers acquired the application development platform that year. Also in 2004, the successor to R/3, the SAP ERP system (or SAP ECC, for SAP ERP Central Component) was released. Customers already using R/2 or R/3 were still supported, but new customers were required to implement SAP ERP. By 2005, SAP was generating $8.5 billion, with upwards of 35,800 employees around the globe.

In 2006, the company claimed hefty revenue from SAP Business All-in-One and SAP Business One, its SAP ERP systems for SMBs.

In 2009, SAP Business Suite 7 became available to customers worldwide. At the time, SAP called it "the company's next-generation software suite enabled by service-oriented architecture."

In 2011, the company launched SAP HANA, an in-memory database platform. HANA was a major development project for SAP, and an important new strategic direction for the vendor, which has said it intends HANA to take the place of the traditional databases SAP has used for its business applications. SAP has offered HANA as a deployment option for Business Suite, and, in 2015, released S/4HANA, an ambitious rewrite of Business Suite optimized for the HANA platform.

As of this writing, Bill McDermott is CEO of SAP, a position he has held since May 2014. In the four years prior, McDermott was co-CEO with Jim Hagemann Snabe. Meanwhile, company co-founder Hasso Plattner is a member of the SAP Supervisory Board and continues to help lead the technology strategy for the company.

3.4 List of SAP Modules and Developing Products

The SAP ERP system, or SAP ECC, is the collective term for SAP's functional and technical modules that enable enterprises to manage business processes through a unified system. ECC is the on-premises version of SAP, and it is usually implemented in medium and large-sized companies. For smaller companies, SAP offers its Business One ERP platform.

SAP ERP has different main modules, which are separated into functional modules and technical modules, each of which has submodules. SAP's functional modules include:

- Human Capital Management (HCM)
- Production Planning (PP)
- Materials Management (MM)
- Project System (PS)
- Sales and Distribution (SD)
- Plant Maintenance (PM)
- Financial Accounting (FI)
- Quality Management (QM)
- Controlling (CO)

SAP also has cross-application components, which can be implemented with any of the main modules. Some of the cross-application components are:

- Document Management System
- Classification
- Product Lifecycle Management

SAP technical modules include:

- Basis
- ABAP
- SAP NetWeaver
- IS (Information Systems) Management
- XI (Exchange Infrastructure)
- Business Intelligence (BI)
- Business Warehouse (BW)
- SAP HANA

Further, SAP also has industry-specific applications that support business processes unique to a particular industry. Some of these applications are:

- SAP for Utilities
- SAP for Insurance
- SAP for Oil and Gas
- SAP Healthcare

SAP Business Suite is a bundle of business applications that provides integration of business and processes, as well as industry-focused functionality. It has SAP ERP as its foundation, plus modules for customer relationship management, product lifecycle management, supply chain management and supplier relationship management. SAP customers can choose to run Business Suite on SAP HANA, its in-memory platform for processing large volumes of data in real time.

3.5 SAP Infrastructure

SAP is an enterprise resource planning system designed to automate and integrate the majority of the Department's business processes by sharing common data and automating routine transactions based on programmable system modules. As of the completion of our audit, the Department had upgraded to and was running SAP ECC 6.0, the most current version of SAP. The Department has deployed the SAP system in a Microsoft environment and is currently running Microsoft Server 2003 and Microsoft SQL Server 2005 on its primary production server. To effectively manage the security and availability of SAP, it is important that information system controls be established and implemented at each tier or layer of the system's architecture. As shown in the figure on page 4, SAP is based on a three-tiered client/server model that includes the following tiers:

- **Presentation Server (SAP Graphical User Interface).** After a user logs onto a Department computer, the user clicks on a desktop icon or selects the appropriate menu path to access the SAP Graphical User Interface, which accepts user input and sends requests to the application server to be processed. The application server processes the user's requests and sends the results back to the SAP Graphical User Interface to format and properly display the results for the user.
- **Application Server.** The application server collectively interprets SAP's Advanced Business Application Programs. These programs are typically grouped within modules that reflect the business functions they are designed to automate, such as financial accounting, human resources, procurement, and payroll. If an Advanced Business Application Program needs to interact with the SAP database, the application server will format the request and send it to the database server.
- **Database Server.** The database server is the part of the SAP system where the actual data related to the various program modules reside. The database server is responsible for processing requests submitted by the application server to add, retrieve, or modify SAP data.

The following diagram depicts SAP's client/server model.

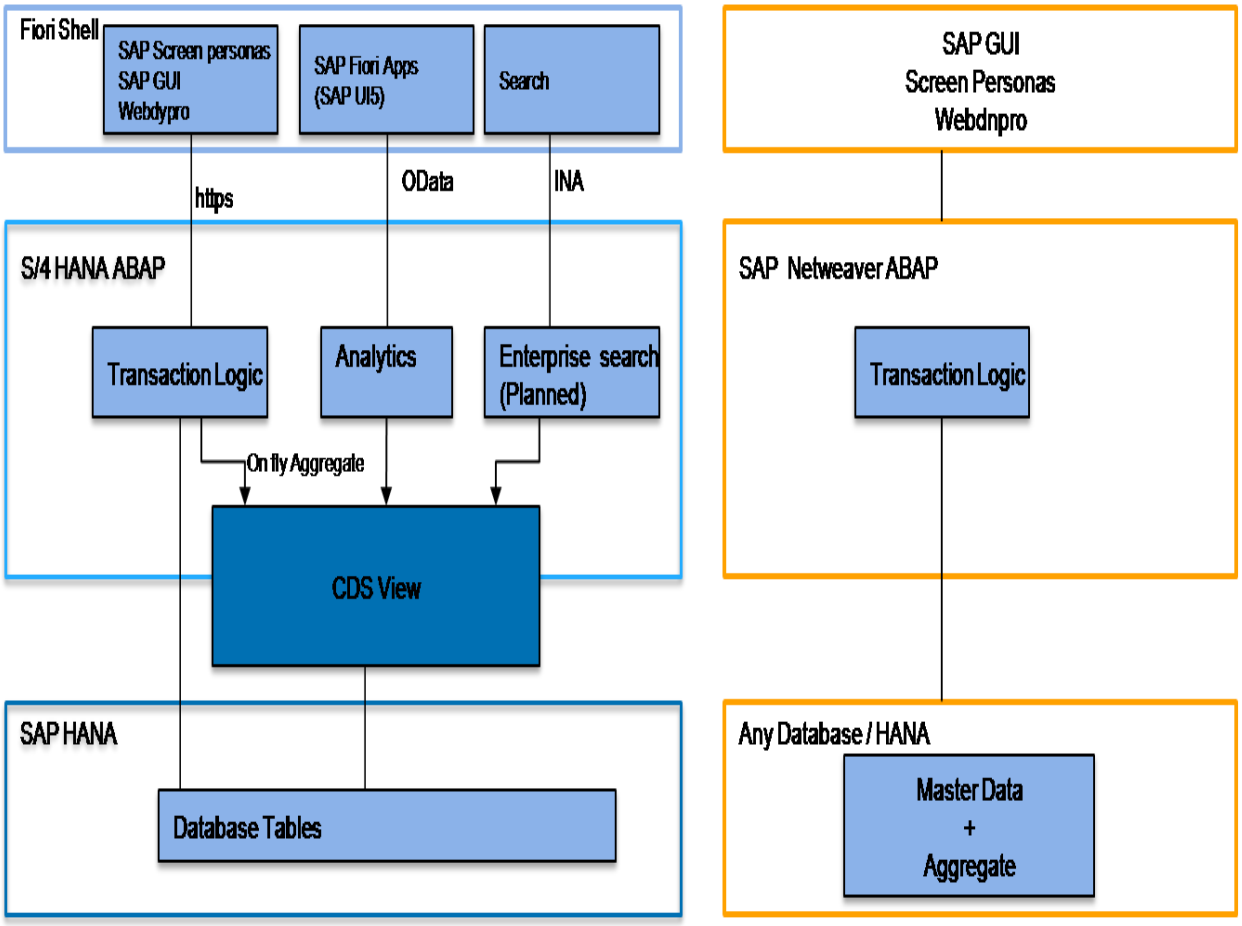

Figure 1: SAP Client Server Model

3.6 Department and OIT Management and Oversight

SAP is maintained and supported by 24 FTE who report through different Department IT business support groups to the Department's Chief Information Officer (CIO). With the passage of Senate Bill 08-155, the Department's CIO reports directly to the Agency Services Director at the Governor's Office of Information Technology, who in turn reports to the State Chief Information Officer (State CIO). Although OIT has oversight responsibility for the Department's IT systems, the Department maintains responsibility for funding SAP operations and providing the strategic direction or identifying the business needs for future SAP enhancements. On July 1, 2010, all Department IT staff will be transferred to OIT as part of the statewide IT consolidation initiative under Senate Bill 08-155.

The following is a brief description of the different work groups and organizations supporting SAP. These groups and organizations are listed:

- **State CIO (OIT):** administrative head of OIT responsible for the management, administration, and oversight of state agency information technology resources, such as SAP, and other IT projects.
- **Agency Services Director (OIT):** member of OIT's Executive Leadership Team responsible for overseeing the IT services provided to each state agency.
- **State Chief Information Security Officer (OIT):** responsible for establishing and enforcing State Cyber Security Policies, network monitoring, vulnerability and threat identification and mitigation, and incident response.
- **Department CIO:** head of all IT operations at the Department, including the support, maintenance, development, and operation of the SAP system. The Department CIO reports to the OIT Agency Services Director.
- **Department Deputy CIO:** responsible for providing, managing, and maintaining the technology infrastructure for the Department, including non-SAP application design and development, workstation and network support, and vendor management. The Application Development (non-SAP), Infrastructure Operations, and Information Security groups report directly to the Department's Deputy CIO.
- **SAP Project Management Office and Business Process Support:** promotes overall project management for SAP, including configuration management, training, and vendor management, and functions as a liaison between the Department's information technology and business divisions. The SAP Project Management Office and Business Process Support report to the Department CIO.
- **SAP Application Development Group:** responsible for the development and maintenance of the SAP Advanced Business Application Programs and interfaces with other information systems such as COFRS and CPPS. The SAP Application Development Group reports directly to the Department's CIO.
- **Affiliated Computer Services, Inc. (ACS):** Department contractor responsible for the development and maintenance of SAP programs and for training Department staff on the use and support of SAP.

3.7 Management of User Access

The second significant deficiency we identified concerns the need for the Department to improve controls over who has access to its systems and data, as well as what actions they can perform. In total, the Department is responsible for managing 4,275 network IDs and 3,181 SAP user IDs. Access management entails managing who has access to specific information, ensuring the access is directly relevant to a particular job or function, and controlling and monitoring user access. User access to SAP and the Department's network must be tightly controlled and managed because of the critical nature of the information processed by the application and transmitted over the network. State Cyber Security Policies require state agencies to provide

users only with the least amount of access necessary to perform their job duties and to establish procedures to ensure that IT security administrators are immediately notified when an employee resigns or is terminated. Additionally, state agencies are required to immediately remove all system access belonging to terminated employees.

3.8 User Access

To access the SAP application, users must complete an access request form that is signed by their supervisor. The request form designates the applications and level of access to be granted. Once signed by the user's supervisor, the form is forwarded to the IT Security Operations Group. The IT Security Operations Group is then responsible for adding the user to the system and assigning the appropriate roles or system access levels. Once a user has been issued valid credentials, he or she must log on or authenticate first to the Department's network and then again to the SAP application. Each time a user logs on, the user must provide his or her authentication credentials consisting of a valid username and password, to gain access.

We reviewed the Department's controls related to user identity and access management and identified the following deficiencies.

Access authorization. State Cyber Security Policies require that all access to state systems be authorized by management and that written records of access requests, changes, terminations, and transfers be retained for one year after the term of the user's employment. We tested the Department's controls to determine if they ensure access to SAP is consistently authorized by management. We selected a sample of 25 SAP user IDs created during Fiscal Year 2009 and requested documentation of management approval for the levels of access granted to these users. We found that Department personnel were unable to locate forms showing management approval for 16 (64 percent) of the SAP user IDs sampled. We interviewed Department staff and determined that IT security staff do not always require a completed access request form prior to setting up a user on the Department's network or in SAP. IT security staff will establish users based on requests received via e-mail or the phone. This practice violates State Cyber Security Policies and increases the risk that an individual may gain unauthorized or inappropriate access to Department computer resources.

Periodic user access reviews. According to State Cyber Security Policies, state agencies are to develop procedures for periodically reconciling lists of terminated users with active user accounts on agency IT systems to ensure that terminated employees' user access credentials have been revoked. Additionally, agencies are required to periodically review all active network and SAP system user accounts to validate that the IDs are still necessary and that users have the appropriate levels of access for their current job duties. Our audit found that Department staff do not perform periodic user access reviews. This has resulted in the following problems:

- **IDs belonging to terminated users.** We evaluated all of the active network and SAP user IDs to determine if active IDs belonging to terminated users existed. Of the 4,275 active network IDs, we identified 20 belonging to terminated users. These network IDs were

active from 28 to 1,139 days since the user's termination, an average of 383 days. Of the 3,181 active SAP IDs, we identified nine belonging to terminated users. These SAP IDs were active from 99 to 121 days since the user's termination, an average of 105 days.

- **Inactive IDs.** We also reviewed controls related to the monitoring of inactive or unused IDs and noted that of the 4,275 network IDs, 182 (4 percent) had been activated but never used. To determine how long these IDs have been unused, we compared their creation date to the date we reviewed them and noted some as old as nine years. Out of the total network IDs, 855 (20 percent) of the IDs had not been used in at least 60 days. Inactive or unused IDs provide attackers an unnecessary avenue for compromising state systems. Inactive IDs should either be set to automatically suspend after a given period of time or be disabled manually by Department IT security staff.
- **Generic IDs.** We also found 474 (11 percent) generic network IDs. Generic IDs are active IDs with no identifiable owner. Generic IDs represent risk in that there is no one who can be held accountable for the activity performed through them. Department IT security staff should review these IDs to determine if they are still necessary. If not needed, these IDs should be immediately disabled. Additionally, for those generic IDs that are needed, IT security staff should identify the ID's owner and add this information to the authentication server.

Password parameters. State Cyber Security Policies require that passwords be a minimum of eight characters, be changed at least every 60 days, and be complex (i.e., a password should contain a combination of capital letters, lowercase letters, numbers, and special characters). We identified problems with both the Department's network and SAP password parameters. For the Department's network passwords, we found that the default configuration settings complied with State Cyber Security Policies. However, in analyzing individual network IDs, we found that the default password configuration settings were routinely overridden by Department IT security staff. Specifically, of the 4,275 network IDs, 999 (23 percent) had passwords older than 60 days, and 187 (4 percent) had passwords that were set to never expire. Additionally, we found that Department IT security administrators had misconfigured the password settings for 993 network IDs. This misconfiguration made it possible for an IT security administrator to reset the password for these IDs to a null or blank password; in other words, no password would be required.

For the SAP application, we found that the Department's default password parameters do not comply with State Cyber Security Policies. SAP passwords have a minimum required length of six characters instead of eight; passwords are only required to be changed after 300 days instead of 60 days; and password complexity is not enforced. Additionally, the SAP application is not configured to prevent users from recycling previously used passwords or from using a password very similar to the one previously used.

The Department's inadequate network and SAP password parameters make it easier for attackers to guess passwords and gain inappropriate and unauthorized access to computing resources and Department data. To prevent password guessing attacks from being successful,

the Department needs to ensure all password parameters comply with State Cyber Security Policies, including those for both the primary authentication server and SAP.

3.9 SAP User Profiles

In SAP, security is implemented by controlling a user's access to tables within the system. SAP is comprised of thousands of tables in which data are stored. Users interact with these tables through the SAP Graphical User Interface. Based on the privileges, or level of access, associated with the user's ID, the SAP system will either process the user's request (e.g., create a new vendor record) or deny it and display an error message. Instead of creating custom privileges for each user, the Department has implemented a role-based access control system. Basically, users who share the same role within the organization are assigned the same system privileges or user profile.

We tested the appropriateness of SAP user profiles related to the module that tracks and processes Department expenditures. We focused on the expenditure module because this module processes over $1 billion in payments annually and because of the risk of errors or fraud if access controls are inappropriate. For example, SAP user profiles should not allow the same person to both add or modify vendor information and to both initiate and approve a payment. Such levels of access could enable a user to circumvent manual controls and allow unauthorized payments to be made.

Overall, we found that the Department has not evaluated SAP user access profiles and identified and documented those profiles, or combination of profiles, that are appropriate for different system users. Although SAP user access profiles have not been defined, we used industry best practices and vendor recommendations to assess the appropriateness of SAP users' access to critical expenditure tables, such as the ability to create and approve a purchase order. We identified the following specific problems with inappropriate access.

- **Critical Expenditure Tables.** The Department has 19 IT staff with access to critical expenditure tables, allowing them to perform specific business functions that are not part of their assigned jobs. These excessive access rights were left over from the pre-implementation environment. This level of access is inappropriate and provides unnecessary risk, and should be eliminated. We provided the specific details of this finding, including a complete list of the specific expenditure tables affected, to the Department under separate cover.
- **System Tools.** The Department does not properly control access to and monitor the use of special system tools. Specifically, we found that more SAP users than necessary had access to the S_Query tool. The S_Query tool can be used to develop customized system queries to view SAP's most sensitive data, including human resources, financial accounting, and project pricing data. According to SAP and industry best practices, access to this tool should be extremely limited. During our audit, we found that 42 SAP users had access to the S_Query tool. In discussions with Department staff, we found that the

S_Query tool should be restricted to the SAP administrative team, which is comprised of five staff.

- **Privileged Transactions.** The Department has not restricted or locked access as recommended by industry best practices to the many highly privileged transactions that can be used to modify administrative tables. For example, the use of the SE11 transaction can be used to modify the SAP data dictionary, and the SU10 transaction can be used to add and delete user profiles. This means that it is possible for SAP users to make significant changes to the system that may not be authorized to perform. Unauthorized changes to these critical administrative tables could have a significant impact on SAP and the data it stores and processes. We provided the specific details of this finding, including a complete list of the privileged transactions that should be restricted or locked as recommended by industry best practices, to the Department under separate cover.
- **Privileged Account.** The Department is not properly monitoring and controlling access to a privileged account used by vendors to install upgrades and troubleshoot problems. This privileged account has full permissions to all tables within SAP, including the expenditure module. Failure to properly monitor and control access to this account provides an unnecessary opportunity for disgruntled employees of the Department's vendors or outside attackers to gain full access to the system and perform unauthorized functions, such as viewing or downloading Department employee information.

To determine if the inappropriate access we identified resulted in specific problems, we requested SAP transaction logs for further review and analysis. However, as previously discussed, the Department has not enabled the logging function within SAP. As a result, we were unable to determine the impact of these inappropriate levels of access. The Department's lack of logs that would enable it to monitor user activity exacerbates the risks that result from inadequate controls over user access.

The Department needs to take several steps to ensure access to SAP is appropriate and properly controlled. First, the Department should evaluate SAP user access profiles and identify and document those profiles, or combination of profiles, that are appropriate for different system users. Second, the Department should periodically review SAP users' levels of access and require unit managers to annually validate in writing that such access is still appropriate. Third, Department staff should remove the excess levels of access we identified during our audit and provided to the Department under separate cover. Additionally, the Department should evaluate and restrict access to tools, transactions, and tables and limit vendor access to the privileged SAP user account for only the time period necessary and should log and closely monitor this account's activities.

3.10 Disaster Recovery

The third significant deficiency we identified relates to the Department's inability to recover the SAP system within the time frames specified by Department management should disaster strike. Information system disaster recovery refers to the process of identifying, testing, and evaluating

all of the resources and procedures needed to make specific information system based functions operational after services have been disrupted. Disaster recovery planning is essential if government is to continue providing services in the event of natural or man-made disasters or more routine interruptions, such as localized power failures or data corruption. State Cyber Security Policies require state agencies to develop comprehensive disaster recovery plans for critical applications. Because SAP is used for most of the Department's business processes, the Department considers SAP a critical application. According to the policy, agency disaster recovery plans must include the following components:

- **Roles, responsibilities, and contact information** for the individuals responsible for implementing the disaster recovery plan.
- **Recovery time frames** outlining both response and recovery requirements.
- **Recovery procedures** detailing the ways in which services will be restored and operations returned to normal.
- **Plan training**, to be conducted on a regular basis, for the individuals who have specific roles and responsibilities in implementing the disaster recovery plan.
- **Plan testing**, to be conducted on a regular basis, to ensure services can be effectively restored and any problems addressed.
- **Plan maintenance** to ensure the plan is updated or modified to reflect changes in recovery requirements, time frames, personnel, or other factors. The plan should also include procedures for distributing the plan to stakeholders and notifying them of any changes to it. We reviewed the Department's disaster recovery testing procedures and planning documents for SAP and found two problems. First and of critical importance, the Department has not conducted a comprehensive disaster recovery test of the SAP system. Therefore, the Department cannot ensure that the SAP system could be recovered within an acceptable time frame in the event of a disaster. Second, we found that the Department's disaster recovery plan for SAP is not current and fails to address all critical components as required by State Cyber Security Policies. Specifically, we reviewed the Department's disaster recovery plan for SAP and found that it lacked the following components:
- Evidence of stakeholder approvals.
- Contact information for essential line and management staff.
- Backup procedures, retention cycles, and onsite and offsite backup storage policies.
- Testing strategies.
- Recovery time objectives to guide the timing of the restoration process.
- Hardware and software inventory needed for full recovery.
- Service level agreements for critical hardware and software.

A comprehensive and well-tested disaster recovery plan is needed for the Department to be able to successfully resume operations following a disaster or system disruption. Because key accounting functions depend entirely upon the SAP application, a significant emergency could halt critical functions such as payroll, purchasing, accounts payable, and accounts receivable for

an extended period of time, severely interrupting essential Department functions. The Department should improve its ability to recover from a disaster by performing a comprehensive disaster recovery test within the next year and updating its disaster recovery plan to include all required and necessary components to guide staff through the restoration process.

3.11 Information Security Management

Statute and State Cyber Security Policies require state agencies to develop annual information security plans. These plans are essential to both the Department's and the Governor's Office of Cyber Security's ability to effectively manage state information security operations. The Governor's Office of Cyber Security, within OIT, relies on agency security plans to assess risk of cyber attacks, develop statewide mitigation plans, identify and mitigate known vulnerabilities, and establish budget and resource priorities. According to State Cyber Security Policies, the Department's information security plan is required to contain information about the agency's:

- Organizational structure, mission, and objectives
- Information technology environment
- Risk management procedures
- Information security program
- Incident warning, advisory, and response procedures
- Training and security awareness plans

As part of the planning process, State Cyber Security Policies also require agencies to annually update and submit a Risk Based Gap Analysis and Plan of Actions and Milestones. The Risk Based Gap Analysis is used as a tool to identify the deficiencies in the agency's information security environment. The Plan of Actions and Milestones is the tool used to identify the specific details, resources, and time frame for mitigating these deficiencies. We reviewed the Department's current Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones, and found that these documents were incomplete, were not updated, and did not reflect the Department's current computing environment or level of compliance with State Cyber Security Policies. For example, the Risk Based Gap Analysis lacked up-todate information for SAP, such as information related to management of access privileges, software change control, and data handling. The Plan of Actions and Milestones is incomplete as well, because its accuracy depends directly on the information contained within the Risk Based Gap Analysis. To ensure the Governor's Office of Cyber Security has the necessary information to manage state security operations, the Department should ensure that comprehensive security risk assessments are completed annually and that its Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones, are updated and accurate.

3.12 Security Awareness Training

Information security awareness training is important to an organization's information security strategy. Users are the first line of defense against threats posed by malicious code, disgruntled employees, and malicious third parties. Information system users need to know what an

organization considers appropriate security-conscious behavior and what security best practices they need to incorporate into their daily business activities. Because of the importance of having security-conscious users, State Cyber Security Policies require that all employees, contractors, and users of state systems receive initial and ongoing security awareness training on at least an annual basis. Agencies are to track the completion of this training centrally and require users to attest in writing that they have completed the training and agree with the agency's acceptable use policy. We found that the Department is not complying with State Cyber Security Policies regarding security awareness training. While all new employees and contractors complete initial training, we found that the Department does not provide SAP users with ongoing security awareness training or require that users annually recertify their understanding and compliance with the Department's acceptable-use policy. Additionally, the Department does not provide specialized, system-specific training to Department employees with information security responsibilities, such as those staff charged with establishing and monitoring user access within the SAP system. It is difficult, if not impossible, to protect the confidentiality and integrity of information without ensuring that all people involved in using and managing data have adequate knowledge of the various controls required and available to protect computing resources under their scope of responsibility. Employees who have limited knowledge of security practices can put the Department at risk through bad habits or lack of attention. Raising and maintaining the awareness level of potential security threats is an essential component of an effective overall security strategy. One of the best ways to make sure employees do not make costly errors with regard to information security is to implement organization-wide security awareness training initiatives that ensure employees have a solid understanding of the organization's security policy and procedures as well as industry best practices. This effort should include providing specialized security training for those with assigned information security responsibilities.

4 Methodology

4.1 Data collection techniques - Interview

Interviews are particularly useful for getting the story behind a participant's experiences. We decided to use the interview as data collection techniques for this project. We interviewed Md. Majharul Huda Lizan, Manager, logistics cost control LafargeHolcim Bangladesh Limited, asked him

About SAP, the information system that they use in the organization. SAP is the leading enterprise information and management package. There are so many information system in the market and of their SAP is the most used in medium to large enterprises. SAP is neatly integrated business software to process all functionalities of an organization in order to obtain a UNIFIED solution, ERP software. SAP is a leader when it comes to easy integration among all the departments.

About ERP we found, it is the term used for software that controls whole organizations different departments. Considering a large enterprise LafargeHolcim, which has of divisions under it. There is a

- Financial Department
- Logistics Section
- Hr
- Warehousing
- Sales and distribution

All these need to be integrated together, for effective functioning. This is done by a specific software known as Enterprise Resource Planning or ERP. Using of this package makes it is possible to track and manage, in real-time, sales, production, finance accounting and human resources in an enterprise.

What makes SAP different?

- Traditional computer information system used by many businesses today have been developed to accomplish some specific tasks and provide reports and analysis of events that have already taken place.
- Occasionally some systems operate in a real time mode that is, have up to date information in them and can used to actually control events.
- A tipical company has many separate system to manage different process like production, sales and accounting.
- Each of those system has its own database and rarely passes information to other system in a timely manner.
- All information system access common data. Real events in the business initiate transactions.
- Accounting is done automatically by events in sales and production.
- Sales can see when production can be delivered.

- Production schedules are driven by sales.
- The whole system is designed to be real-time and not historical.

4.2 Paper analysis

We collect some papers written on SAP information system and gather information about its details procedure.

5 Findings

Table 1: Finding Classification

Definition of Finding Classifications	
Classification	**Description**
Material Weakness	A material weakness produces an immediate risk directly impacting the confidentiality, integrity, and availability of information systems and data. For IT projects, a material weakness represents an immediate threat to the overall success of the project. This would be considered a high risk finding.
Significant Deficiency	Significant deficiencies do not alone produce an immediate risk, but could affect the confidentiality, integrity, or availability of systems in conjunction with other factors. For IT projects, significant deficiencies do not represent an immediate threat to the overall success of the project but could result in project delays, cost overruns, or incomplete deliverables. This would be considered a moderate risk finding.
Control Deficiency	Control deficiencies do not present an immediate risk but could be indicative of operating deficiencies and/or have the potential to adversely affect the confidentiality, integrity, or availability of systems over an extended period of time. For IT projects, control deficiencies may not represent an immediate threat to the overall success of the project but could, over an extended period of time and in conjunction with other deficiencies, result in project delays, cost overruns, or incomplete deliverables. This would be considered a low risk finding.

Table 2: Audit Finding

Rec. No.	**Audit Finding**	**Classification of Findings**		
		Material Weakness	**Sig. Deficiency**	**Control Deficiency**
1	Improve the Department's incident detection, response, and reporting capabilities and practices.		X	
2	Strengthen the Department's access management controls, including ensuring that critical SAP tools, tables, and privileged accounts are tightly controlled and monitored.		X	
3	Update the SAP disaster recovery plan and conduct a comprehensive disaster recovery test.		X	

4	Complete annual risk and vulnerability assessments and update the Department's Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones.			X
5	Ensure Department users are provided annual information security awareness training and are recertifying their understanding and compliance with the Department's acceptable-use policy.			X

5.1 Conclusion

At SAP, their purpose is to help the world run better and improve people's lives. Their promise is to innovate to help their customers run at their best. SAP is committed to helping every customer become a best-run business. They engineer solutions to fuel innovation, foster equality, and spread opportunity across borders and cultures. Together, with their customers and partners, they can transform industries, grow economies, lift up societies, and sustain our environment. Although their system has some lackage and there are some recommendation from their customers SAP is providing one of the best support to Lafarge and other medium and large enterprises.

References

[1] 20 April 2018. [Online]. Available: https://searchsap.techtarget.com/definition/SAP-FICO-SAP-Finance-and-SAP-Controlling.

[2] 20 April 2018. [Online]. Available: https://www.sap.com/corporate/en/vision-purpose.html.