ISO 27000 Framework

ISMS

COS7030-B

CASE STUDY ABC Technologies

This case study has been developed by PECB

Company History

ABC Technologies is the new name of ABC Printing. Paul Evans (President) and Sally McCarty (Executive Vice-President) created ABC Printing in 2011 at the end of their university studies. The Yorkshire company saw rapid expansion. It had 253 employees in 2016 when Paul and Sally decided to diversify their activities by venturing out into 3D graphics printing. This activity, then emerging with the development of information technologies, was supported by both senior executives who saw in it the means to strike a balance between their traditional activities and what they considered the future of the printing industry.

These longtime friends are enthusiasts of new technologies. They have always known that the information technology sector had a great growth potential. Conscious of the importance of information and technologies, Paul and Sally seized an opportunity offered them in 2016: A&B Technologies, a company that developed and commercialised Customer Relationship Management (CRM) software, and that was located about a hundred meters from their premises, went bankrupt. Since their printing and computer graphics activities generated cash surpluses, they decided to buy out A&B Technologies. ABC Printing was then renamed to ABC Technologies to display an image more in line with its new field of activity. The merging of ABC Printing and A&B Technologies produced a company with 567 employees distributed as follows: 556 employees in the printing and 3D graphics divisions, and 11 employees in the CRM division.

The software developed by A&B Technologies facilitates the acquisition of information, including customer data entry (name, contact information, availability, recreation). It allows a company to store, control and modify information, plan tasks, annotate notifications as well as several other functions. Three products are distributed: ABC Supreme (£3,995), ABC Pro (£495) and ABC (£295).

ABC Technologies' head office is located in Bradford. This location combines the printing, 3D graphics printing and software development activities.

Following the growth of the company, another office was opened in Leeds in 2012.

Paul Evans decided to take charge of the Leeds office, where sales and services are managed. Since these involve a strong need for managing customer relations, he was the best candidate for the job thanks to his communication and negotiation skills. Administration team was also located in Leeds.

Sally McCarty stayed in Bradford to manage software development, printing, 3D printing graphics, and IT services because of her technical competencies.

To finance the growth of the company, ABC Technologies concluded an investment agreement of over 2 million dollars with a capital investment fund. With this agreement, investors insisted that ABC restructure the company governance by having a formal Board of Directors and hiring an experienced CEO. Sabina Senat was hired as CEO to manage all the firm's activities. Known for her outspokenness and her direct actions, Mrs. Senat was involved in the restructuring of several start-ups.

Since the take-over of A&B Technologies, business is booming. The software activity has made important sales thanks to various distribution channels which include direct sales, indirect sales (partnerships), as well as recent web sales. Unfortunately, the growth of the software activity has produced serious management, organization and operation problems. These problems include the loss of important information, the loss of several contracts, and more important still, the loss in confidence of some customers. In addition, the number of new competitors and similar products on the market has rapidly increased, and has started to slow the growth of the company's software activity.

In light of these developments and to regain the confidence of their customers, Sabina Senat, Paul Evans and Sally McCarty decided to implement the ISO/IEC 27001 standard and to get certified.

ABC Technologies Facilities

Head Office (Bradford)

All the employees have desktop computers connected through a network and operating with Windows 10 operating system. The network is connected to a central file server. This server is used to store all relevant information, such as orders sent by email in PDF format from the Leeds office, production records, personnel data, and the information on the design of products.

Sales Office (Leeds)

The Leeds office has the same configuration as the head office. The personnel use desktop computers that operate with Windows 10. The network is also connected to a central server, which is used to store customer data, customer orders, financial and accounting records, and contracts of partnerships. The sales team is concentrated in this sales office under the supervision of Owen Roger. And, all orders are transferred by email to Paul Evans who is in contact with Sally McCarty for deliveries.

IT Network

The head office system and IT network are managed by William Clay, IT Manager, Peter Ly, Network Supervisor, and Fred Jones, Helpdesk Supervisor. Billy Davis, the Helpdesk Technician at Sales Office, manages the network and the helpdesk, and writes and sends monthly reports to Fred Jones, as do Helpdesk Technicians at Head Office.

Recent Facts and Events

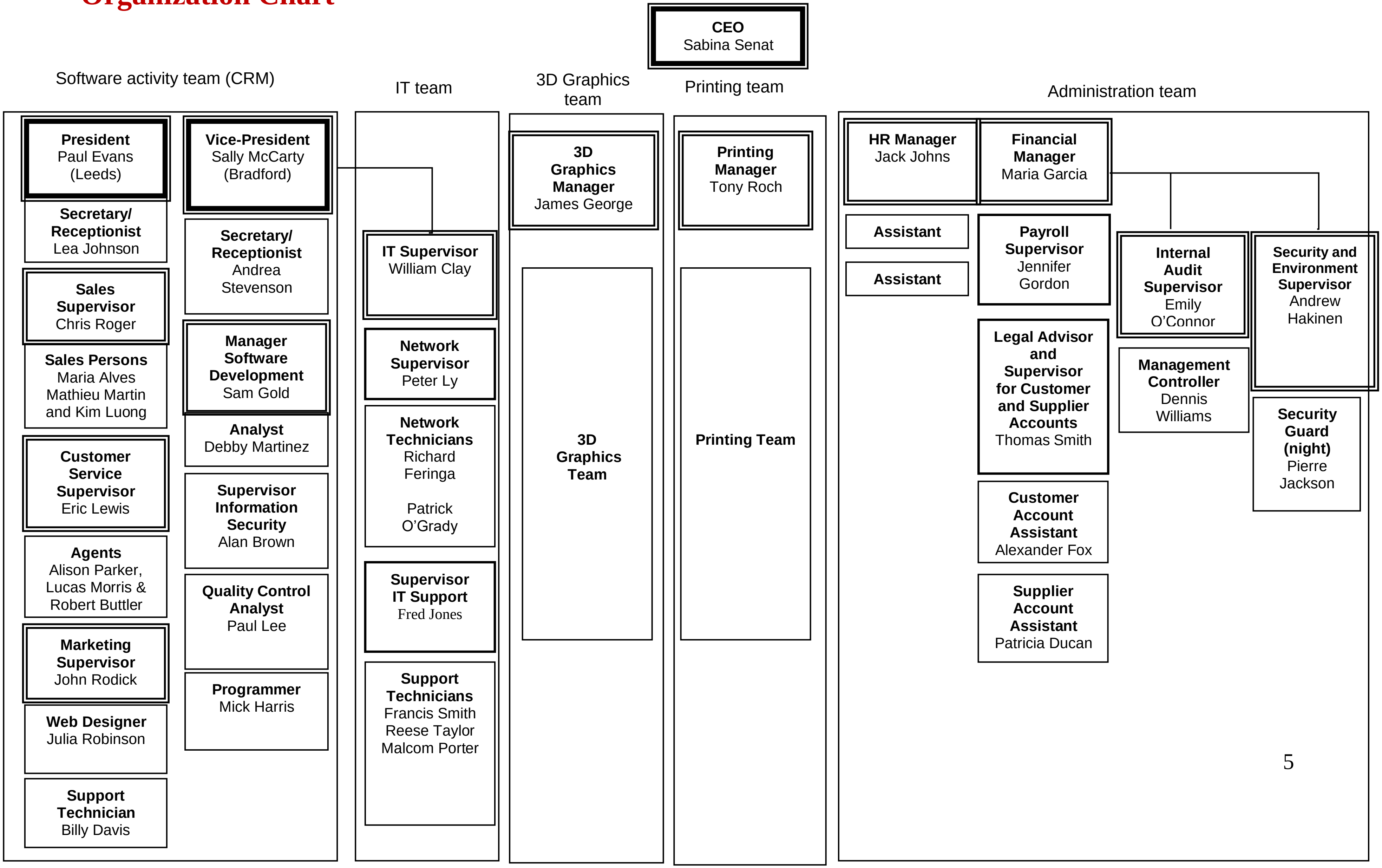
After the arrival of the new CEO, Mrs. Senat, the following employees were fired:

- Peter Campbell, previous CEO
- Ian Kovalev, Accounting VP
- Katie Harper, Marketing Assistant

Additionally, the following events took place:

- The Bradford office alarm system does not work and the company that installed it went bankrupt two months ago
- Julia Robinson, the website designer, was sick for one month
- Eric Lewis was informed by a customer that Steven Baker and Ian Kovalev were hired by their competitor, BearClan
- Personal information on customers is kept in a database with no security measures in place to protect it
- Although a formal description of the employees' roles and responsibilities exists but, several employees perform additional tasks and do not adhere to the document
- ABC Technologies has bought a list of 500,000 emails of potential customers from a company located in the Bahamas to launch an Internet advertising campaign
- A corporate website of ABC Technologies was built by a website development company that also took responsibilities of relevant updates.

Organization Chart



CEO
Sabina Senat

Software activity team (CRM)

President
Paul Evans
(Leeds)

Secretary/ Receptionist
Lea Johnson

Sales Supervisor
Chris Roger

Sales Persons
Maria Alves
Mathieu Martin
and Kim Luong

Customer Service Supervisor
Eric Lewis

Agents
Alison Parker,
Lucas Morris &
Robert Buttler

Marketing Supervisor
John Rodick

Web Designer
Julia Robinson

Support Technician
Billy Davis

Vice-President
Sally McCarty
(Bradford)

Secretary/ Receptionist
Andrea
Stevenson

Manager Software Development
Sam Gold

Analyst
Debby Martinez

Supervisor Information Security
Alan Brown

Quality Control Analyst
Paul Lee

Programmer
Mick Harris

IT team

IT Supervisor
William Clay

Network Supervisor
Peter Ly

Network Technicians
Richard
Feringa

Patrick
O'Grady

Supervisor IT Support
Fred Jones

Support Technicians
Francis Smith
Reese Taylor
Malcom Porter

3D Graphics team

3D Graphics Manager
James George

3D Graphics Team

Printing team

Printing Manager
Tony Roch

Printing Team

Administration team

HR Manager
Jack Johns

Assistant

Assistant

Financial Manager
Maria Garcia

Payroll Supervisor
Jennifer
Gordon

Legal Advisor and Supervisor for Customer and Supplier Accounts
Thomas Smith

Customer Account Assistant
Alexander Fox

Supplier Account Assistant
Patricia Ducan

Internal Audit Supervisor
Emily
O'Connor

Management Controller
Dennis
Williams

Security and Environment Supervisor
Andrew
Hakinen

Security Guard (night)
Pierre
Jackson

Implementation of the ISMS

To prove ABC Technologies' competence in information security and gain greater confidence from its customers, you have been employed as a consultant by Sally McCarty to implement the ISO/IEC 27001 prerequisites to obtain certification.

The implementation of ISO/IEC 27001 is done by creating an ISMS. You must firstly formally define and clarify the scope of the ISMS, however, with this in mind, it has already been decided that only ABC Technologies' **software activity** would be included in the ISMS. During a meeting with Sabina Senat and the persons in charge of the software activity, it was estimated that the information to protect was:

- the product development plan (design, development costs, source code, etc.),
- the marketing plans (the company's development strategy),
- the human resources data,
- the customer database,
- the financial and accounting data,
- all contracts (partnerships, employees, contractors).

The information assets considered to be **the most important** are the **product source code**, and the **company financial and accounting data**.

To account for the external threats, the managers have extended the ISMS scope by incorporating SoftProd, a database which contains information on ABC's products, and the companies in charge of maintenance on both sites.

You must take into account that each employee can connect to the network from anywhere, through an Internet connection, using their own login and password thanks to a VPN.

Following the clarification of the ISMS scope, you should create:

1. Formative and Final Scope
2. Formative and Final Risk Assessment following OCTAVE Allegro. Please focus on **one critical asset** in Worksheet 8 and **three areas of concern** in Worksheets 10.
3. Statement of Applicability
4. Document Development:
    a. Background Terms
    b. Master List of Documents
    c. Remote Access Policy and three policies of your choice to show you understand the steps needed to implement your complete ISMS

Additionally, please write Introduction (as a general introduction to a document)

The key to this assessment is the reflective narrative related to academic literature around the development of your ISMS. You can structure this such that you reflect on each stage or that you have a reflective piece that encompasses all you have developed.

You must make assumptions about some components of the ISMS if this information is not available in the case study, but you need it for the effective implementation of the ISMS.

Looking at the Plan-Do-Check-Act cycle, you must decide the appropriate order to carry out the tasks. However, you must make sure you clarify ABCs attitude to risk and therefore establish the risk treatment plan (transfer, avoidance, acceptance, or reduction). The ISMS policy has been developed and is below for clarification of the objectives.

ISMS Policy

- **Statement**

- The object of this policy is to define the policy of the Information Security Management System for ABC Technologies.

- **Definitions**

- **Information Security Management System (ISMS):** Part of the total management system, based on a business risk approach, allowing to establish, implement, operate, control, review, maintain and improve information security.
- **Information Security** is the protection of information from a set of threats to ensure business continuity, reduce business risks to a minimum, and maximize the return on investment and business opportunities.

- **Scope and Application**

- The current policy applies to all Users. The use of Information Assets by a User constitutes in itself an implied acceptance of the policy.
- It is up to the Support Department Manager, in cooperation with ABC Technologies Management, to ensure the respect of this policy and to take the necessary measures to apply it.

- **Objectives**

- Clarify the organization’s security strategy.
- Ensure that the appropriate information and critical actions are protected from threats.
- Ensure that, in case of system error or any other threat, all the appropriate information and critical assets maintain a satisfactory level of confidentiality, integrity and availability, as determined by management.
- Ensure that, in case of error, disaster or any other problem that can threaten ABC Technologies, ABC’s commercial operations continue to operate with a minimum degree of obstruction.
- Create a security culture involving employees.

- **Policy**

- The policy must be approved by management.
- All the critical information of ABC Technologies, which includes: the data stored on computers, the information transmitted over the networks, printed or written on paper, sent by fax, stored on cassettes or diskettes, or transmitted verbally in conversations or over the telephone must be protected from any threat whether it be internal or external, deliberate or accidental.
- Any authorization for access to information given to a person must be defined and approved by the person’s supervisor.
- Vital information and services must be available to authorized users when and where they need them with the lowest level of interruption possible.
- Information integrity must be maintained, and its exactness and completeness must be ensured to protect it against changes and unauthorized accesses.
- Information confidentiality must be ensured. The date of human or electronic communications must be protected to ensure that valuable or sensitive information is protected against unauthorized disclosures or inevitable interruptions. The organization must conform to all the IT sector regulatory and

legal specifications to avoid any fines or financial costs caused by nonconformity to the law.

- A management framework of business continuity must be provided using a business continuity plan to counter business activity interruptions and to protect the critical business processes in case of disaster. The business continuity plan must be maintained, tested and reviewed to be efficient in case of an event that can cause damages to ABC Technologies.
- ABC Technologies must train its employees on information security by putting in place a continuous awareness program on the importance of information security and the participation to the necessary trainings.
- Real or suspected security breaches must be evaluated and reported to the competent authorities.
- Adequate access control must be put in place and the information must be protected against unauthorized accesses.
- To support the ISMS, all policies, procedures and guidelines must be available in print or electronic version to all authorized persons by means of an internal network system (intranet).
- All supervisors are responsible for implementing the ISMS in their Department.
- All personnel have the responsibility to adhere to the ISMS policy.
- In case of an information security problem, the situation must be handled using ABC's risk management framework.

ABC	Title: ISMS Policy	No: MTR-POL
		Revision Date: January 2019
		Number of pages: 3
Issued by Alan Brown	Division: ABC Technologies	Approved by: Paul Evans

Additional Notes

1. Software developed by ABC Technologies is held in a Software-as-a-Service (SaaS) environment provided by ABCloud. Although the organization has signed ABCloud's standard terms and conditions, it is unclear what security requirements ABCloud must fulfil. It is understood that ABCloud have data centres in the UK, USA and India and some personal data may therefore be held on ABCloud servers in these countries
2. Although policies have been developed, it is not clear when or if they have been reviewed and what the process is
3. Sally McCarty's laptop was stolen from a train station last week
4. It has become clear that Jennifer Gordon's contract for employment was not signed. It isn't clear if she was even aware that she had to sign it. If she was to leave, ABC Technologies would be in difficulty as nobody knows how to do her job and she wouldn't have to give a period of notice
5. ABC Technologies have had a recent office move and printed copies of source code were left on the floor for the cleaners to move
6. The asset register is very basic, and it is not clear if this is up to date
7. Contingency plans for when people are off sick or leave need developing
8. An access control policy was never developed
9. Physical access control is outsourced as the premises are managed by the leasing company
10. A clear desk policy is in operation, but staff members are still leaving paperwork out over the evening and at weekends
11. Staff members also work from home and need remote access at times. Some work needs to be done around removing equipment and what is and is not allowed
12. A clear policy and suitable environment are needed for development and testing of software

13. It isn’t clear if backups have ever been tested
14. The company has efficient and effective logging and monitoring activities. All are kept up to date, reviewed appropriately and stored securely
15. Installation of software and the integrity of operational systems are maintained effectively
16. Network segregation needs clarification
17. The company needs to spend some time developing useful transfer policies and procedures. Staff don’t know what it is acceptable and what is not
18. As the company wants to focus on software development, the company needs to ensure that information security is applied to the complete development lifecycle. This needs to be embedded in all aspects (from initial planning to testing)
19. Supplier relationships and contracts are key; clarification with suppliers and their part in ensuring security of information is essential. Contracts are in place, but these don’t include all the necessary activities. In particular service delivery needs to become better controlled
20. Only the important incidents related to the network are documented and discussed during the IT team’s weekly meeting
21. The last review of security controls took place 18 months ago
22. The organization assumes it complies with all legislation, but there isn’t a definitive list of applicable legislation
23. The review of compliance with policy, standards and procedures is overdue. A timeframe has never been fixed but managers appear to do this when incidents happen.