POLITECNICO
DI TORINO

Master of Science in

Mechatronic Engineering

Thesis

Re-engineering and automation of a Enterprise Risk Management program

Supervisor: Prof. Marco Ghirardi

***Student*:** Damiano Renzetti

July 2018

Index


POLITECNICO DI TORINO
1859
1906

I. Foreword

It might sound atypical, uncorrelated or uncommon for an automation engineer to be conducting a curricular internship in a Finance Management position.

It has been actually very interesting and enjoyable to bring the expertise and technical capabilities gained through Polytechnic University of Turin “Master of Science in Mechatronic Engineering” course of studies, into the Finance department of a multinational corporation like Bruker. The fact that the internship was carried out in the United States of America, the biggest economic power in the world, made everything look even brighter and more attractive. I always have been fascinated by the Business and Management roles and their duties. Getting to know how a corporation of such dimensions is controlled from an operational and financial point of view and perspective, is captivating. One may be questioning how a very technical engineer could be helpful, or how does he catch-up with the knowledge on Finance and Audit, the US laws and regulations, the language and terms that fellow accountants are more familiar with.

This document is going to walk the reader through the experience of being an “Internal Controls Intern" in the USA, starting from the beginners guide of the Risk Management knowledge, just like I did when I was hired for this role.


POLITECNICO DI TORINO
1859
1906

II. Introduction

(1) Company and Internship

1. Bruker Corporation

The Bruker Corporation is a multinational company, a manufacturer of scientific instruments for molecular and materials research, as well as for industrial and applied analysis.
It is headquartered in Billerica, Massachusetts and is the publicly traded parent company of Bruker Scientific Instruments (Bruker AXS, Bruker BioSpin, Bruker Daltonics and Bruker Optics) and Bruker Energy & Supercon Technologies (BEST) divisions.

History[1]

Fig.1 - Bruker Logo

The company was founded on September 7, 1960, in Karlsruhe, Germany as Bruker-Physik AG from Günther Laukien, who was a professor at the University of Karlsruhe. The name Bruker originates from co-founder Emil Bruker, as Günther Laukien himself was formally not allowed to commercialize his research projects while being a professor. Bruker produced Nuclear Magnetic Resonance Spectroscopy (NMR) and EMR spectroscopy equipment at the time. In the early 1960s, the company had around 60 employees and was growing rapidly. One of the early success products was the HFX 90 NMR spectroscopy system, with three independent channels and which was also the first NRM system using only semiconductor transistors. In 1969, Bruker launched the first commercial Fourier transform NMR spectroscopy system (FT-NMR) and in the 1970s the company was the first to commercialize a superconducting FT-NMR. Later, the company expanded the product range with MRI, FTIR and FT-Raman spectrometers and with mass spectrometers. In 1968, Bruker shipped NMR systems to Yale University in Connecticut. After that, demand from the United States grew, so Bruker opened an office in Elmsford, New York which was the start of their US activities. In 2008 after a corporate reorganization lasted 8 years, all divisions were merged in a unified Bruker Corporation. Günther Laukien died in 1997, his son Frank D. Laukien, is currently the CEO of Bruker.

Main acquisitions of Bruker[1]

- Siemens AXS (1997)
- Nonius (2001)
- MacScience (2002)
- Vacuumschmelze Hanau (2003)
- Röntec (2005)
- SOCABIM (2005)
- PGT (2005)
- Keymaster (2006)
- Quantron (2006)
- JuWe (2008)
- SIS (2008)
- ACCEL (2009)
- Michrom Bioresources (2011)
- Skyscan (2012)
- Prairie Technologies (2013)
- Oncovision (Preclinical PET imaging business, 2016)
- Hysitron Inc. (2017)

Products Range[1]

Bruker develops and delivers a wide variety of professional and scientific analysis devices, including:

- Mass spectrometers
- X-ray diffractometers
- X-ray tomography devices
- NMR spectroscopy devices
- Fluorescence microscopes
- Raman spectroscopes
- Atomic-force microscopes
- Profilometers

From the organizational point of view, Bruker Corporation is very complex.
The chart here below shows how the legal entities are organized.

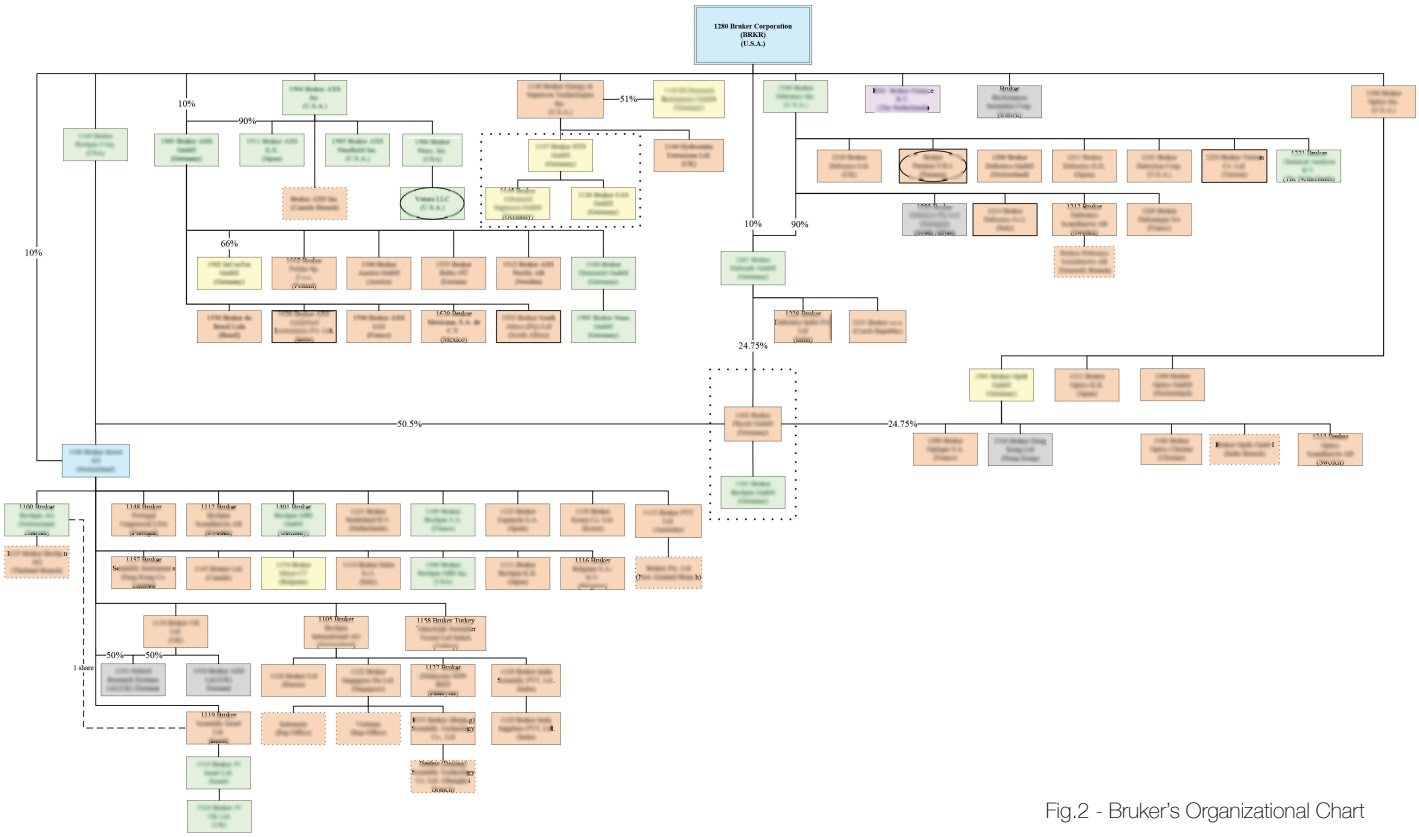


Fig.2 - Bruker's Organizational Chart

Only the circled entities (two out of 88 active entities) are not in the scope of US Sarbane Oaxley (SOX) Act. The management of the SOX compliance program is part of the Internal Controls team duties. This chart gives an idea of the complexity of the Internal Controls organization and of the Corporation itself. It doesn't report the companies names and internal codes to protect the sensitive information, but it gives an idea of the difficulties to face in order to measure internal controls efficiency.

The internship was carried out in the Headquarter of Bruker Corporation in Billerica (MA), USA, (Fig.3) and in the subsidiary located in Berlin, Germany during a business trip to rationalize the German legal entity Internal Control structure.

2. Internal Controls Intern role

This section of the document is meant to explain the role I was assigned in Bruker, while performing the internship.

"The primary responsibility of this position is to drive implementation of financial governance processes at Bruker Corporation, with the goal of creating a compliant and audit-ready organization. To ensure readiness, the Internal Controls Staff intern assists the Sr. Manager – Internal Controls in evaluating governance, business unit risks and financial controls, driving the pre-audit assessment in collaboration with the Internal Audit team and management. The Internal Controls Intern works as a collaborative partner with Group management and business units from both a technical and managerial point of view and periodically reviews the control environment to measure control performance and adequacy of evidence, in order to ensure that the environment stays compliant.

The Internal Controls Staff Intern reports directly to the Senior Manager – Internal Controls.

Responsibilities

The Internal Controls Intern works with global teams from Finance, IT, Operations, Sales, Services and business unit professionals that bring together the full range of technical and business competencies needed to assist Senior Management with the successful achievement of risk mitigation, and compliance with Sarbanes-Oxley.
The individual acts as a technical partner and supports the Internal Controls team in providing oversight on all aspects of translating compliance requirements into controls.
Software platforms such as SAP and Workiva - Wdesk need to be used and managed.
This role interfaces with all levels of management and employees within the European geographic areas, so the Internal Controls Intern has excellent communication skills.

The Internal Control Intern works with the management teams to evaluate and document the design and effectiveness of the automated and non-automated control environment, assists in the development of remediation efforts when necessary and reports on compliance results.

Responsibilities also include

- Support project management of internal testing at subsidiary locations;
- Assist in reviewing test work papers;
- Provide support with developing procedures to insure robust control;
- Assist senior management in identifying control gaps and associated remediation plans;
- Track and trend remediation efforts and overall compliance with operational standards;
- Report and recommend improvements in compliance processes;
- Perform other duties as required."[2]

The Internship description is an interesting mix between Management and Engineering, in the world of Finance and Risk Management. What I found thrilling while working at Bruker is the cooperation with top management teams and the company chief officers. Strategic thinking, project management and team work at their finest were the key to achieve success.
Team work oriented education was greatly proposed and experienced also at Polytechnic University of Turin, and this confirms the importance of enrolling in a Graduation Program of one of the top universities in Europe.

An insight on the COSO framework (a standard ERM framework) and the Sarbane Oaxley Act (a law on Internal Controls and Risk Management for public USA companies), is given in the next sections of this document.

Fig.3 - Bruker Headquarters - Billerica (MA), USA

(2) Corporate Risk Management

1. Internal Controls

Internal controls are **processes** for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. Risk Management is achieved through Internal Controls testing.

In-fact Internal controls are, as a broad concept, everything that controls risks to an organization or enterprise. They play an important role in protection against fraud and organization's resources assurance, both physical (e.g., machinery and property) and intangible (e.g., goodwill or intellectual property such as trademarks).

For what concerns Finance, Internal Controls objectives are related to the reliability of financial reporting, timeliness of operational and strategic goals, and compliance with laws and regulations (e.g. US GAAP, SOX Act in the USA).

At the specific operational level, Internal Controls refer to the actions taken to achieve a specific objective or any other action that does not impact the financial statements of an organization. Internal Controls procedures aim to create a standard in processes, leading to more predictable outcomes and enhanced repeatability of the controls/operations results.

Internal Controls also are a key element of the United States of America Foreign Corrupt Practices Act (FCPA) of 1977 and the Sarbanes–Oxley Act of 2002. These laws required improvements in the Internal Controls structure of United States publicly traded corporations.

Definitions

There are many definitions related to Internal Controls, as they affect the organization and its stakeholders in various ways, and at different levels of the organizational structure.

Committee of Sponsoring Organizations of the Treadway Commission(COSO) Framework, is the main framework used as a guideline to discipline Internal Controls within an organization and was formed in 1985 from the National Commission on Fraudulent Financial Reporting (the Treadway Commission).

The Treadway Commission was originally jointly sponsored and funded by five main professional accounting associations in the United States:

I. American Institute of Certified Public Accountants (AICPA);
II. American Accounting Association (AAA);
III. Financial Executives International (FEI);
IV. Institute of Internal Auditors (IIA);
V. Institute of Management Accountants (IMA).

The Treadway Commission recommended the joint work of the sponsoring organizations to develop integrated guidance on Internal Controls. These five organizations formed what is now called the **COSO,** Committee of Sponsoring Organizations of the Treadway Commission.

The COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal controls and fraud deterrence.[3] Under the COSO Internal Controls - Integrated Framework, widely used not only in the United States but the whole world, Internal Control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives related to operations, reporting, and compliance.

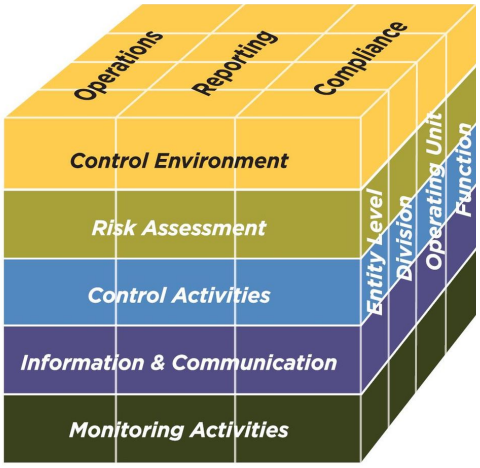


Fig.4 - 2013 COSO Framework cube

COSO defines five Internal Controls components:

(1) **Control Environment:** sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of Internal Control;

(2) **Risk Assessment:** the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed;

(3) **Control Activities:** policies and procedures that help ensure directives are carried out;

(4) **Information & Communication:** systems or processes that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities;

(5) **Monitoring:** processes used to assess the quality of Internal Control performance.

In Deep

Setting objectives, budgets, plans and other expectations is what needed for control purposes. The Internal Control itself exists to keep performance and outcomes within what is expected, allowed or accepted. Controls built within an industrial process are internal in nature. They take place with a combination of interrelated components – such as social, ethic and cultural environment effecting behavior of employees, information, policies and procedures. The Internal Control structure is basically a plan determining how Internal Controls exists, and consists of these elements.[4]

The concepts of corporate governance also heavily rely on the necessity of Internal Controls. Internal Controls processes help ensure that industrial processes operate as designed and that risk management is carried out. In addition, there needs to be in place circumstances ensuring that the aforementioned procedures will be performed as intended: right attitudes, integrity and competence, monitoring by the management machine of the corporation.

Internal controls may be described in terms of:

(a) The objective or financial statement assertion;
(b) The nature of the control activity itself.

(a) Objective or assertions categorization

Assertions are disclosed by the management and embodied in the financial statements.
e.g.: If a Financial Statement shows a balance of $1,000 worth of Fixed Assets, the management asserts that fixed assets actually exist as on the date of the financial statements, the valuation is worth exactly $1000 (based on the reporting framework and standards) and the entity has complete right/obligation arising from such assets.

There are five main assertions:

1. **Presentation and disclosure**: Accounts and disclosures are properly described in the financial statements of the organization;
2. **Existence/Occurrence/Validity**: Only valid or authorized transactions are processed;
3. **Rights and obligations**: Assets are the rights of the organization, the liabilities are its obligations as of a given date;
4. **Completeness**: All transactions are processed fully;
5. **Valuation**: Transactions are valued accurately using the proper methodology, such as a specified means of computation or formula.

For example, a validity control objective might be:

"Payments are made only for authorized products and services received."

And a typical control procedure would be:

"The payable system compares the purchase order, delivery note, and vendor invoice prior to authorizing payment."

(b) Activity categorization

Activities include (but are not limited to):

- **Segregation of duties** – separating authorization, custody, and record keeping roles to prevent fraud or error by one person;
- **Authorization of transactions** – authorization of particular transactions by an appropriate person;
- **Retention of records** – maintaining documentation as evidence of transactions;
- **Supervision or monitoring of operations** – observation or review of ongoing operational activity;
- **Physical safeguards** – usage of cameras, locks, physical barriers, etc. to protect property, such as inventory;
- **IT General Controls (ITGCs)** – Controls including:
  (a) Security, to ensure access to systems and data is restricted to authorized personnel, such as usage of passwords and review of access logs;
  (b) Change management, to ensure new software code is properly controlled, such as separation of production and test environments, system and user testing of changes prior to acceptance, and controls over migration of code into production.
- **IT application controls (ITACs)** – Controls over information processing enforced by IT applications, such as edit checks to validate data entry, accounting for transactions in numerical sequences, etc.

Roles and responsibilities in Internal Control

According to the COSO Framework, everyone in an organization has responsibility for internal control to some extent. Virtually all employees produce information used in the Internal Control system or take actions that affect control. Also, all personnel should be responsible for communicating upward problems in operations, non-compliance with the code of conduct, other policy violations or illegal actions.

Although the responsibility participation begins from the lowest level in the organizational tree, major entities in corporate governance have particular roles to play:

Management

The Chief Executive Officer (CEO) of the organization has overall responsibility for designing and implementing effective Internal Control. More than any other individual, the chief executive sets the **"tone at the top"** that affects integrity and ethics, and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific Internal Control policies and procedures to personnel responsible for the unit's functions. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and commercial/ financial units of an enterprise.

Board of Directors (BOD)

Management is accountable to the board of directors, (corporate governance) which provides governance, guidance and oversight and which role is well distinguished from the Management. BOD members posses knowledge of the corporation activities and environment. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct Internal Control issues.

Auditors

There exists a distinction between Internal Audit and External Audit.
Both the internal auditors and external auditors of the organization measure the effectiveness of Internal Control through their efforts. They assess whether the controls are properly designed, implemented and working effectively, and make recommendations on how to improve Internal Control. They also review Information Technology controls, which are related to the IT systems of the organization.

In the U.S. the regulations on Internal Controls are specifically established by Sections 404 and 302 of the Sarbanes-Oxley Act (treated in the next section of this document). Guidance on auditing these controls is specified in Public Company Accounting Oversight Board (PCAOB) Auditing Standards, and Security and Exchange Commission (SEC) guidance & standards. Internal Auditors initially assess the quality of the Internal Controls structure of an organization providing recommendation to Management. The information escalates to the top (Audit Committee) and remediation plans that take into account auditors findings and recommendations are put in place. The Internal Controls are subsequently tested by the External Auditors (public accountants hired by the organization) to provide reasonable assurance that Internal Controls involved in the financial reporting process are effective. The External Auditors opine on the Internal Controls of the company and the reliability of its financial reporting, publicly reporting outcomes. This cycle takes place every year.

Audit committee

The role and the responsibilities of the audit committee, in general terms, are to:

(a) Discuss with management, internal and external auditors and major stakeholders the adequacy of the organization's Internal Controls system, its effectiveness and outcomes, and meet privately with the Director of Internal Audit;

(b) Review, discuss and approve with management and the external auditors the audited financial statements of the organization, then make a recommendation regarding inclusion of those financial statements in public filing;

(c) Review and discuss with management the information to be disclosed with respect to the Company's earning press release and financial information guidance provided to analysts and rating agencies;

(d) Confirm the scope of audits to be performed by the external and internal auditors, monitor progress, review results, fees and expenses. Review significant findings, audit problems or difficulties encountered by the external auditors. Monitor management's response and remediation plans to all audit findings;

(e) Receive regular reports from the Chief Executive Officer, Chief Financial Officer and the Company's other Control Committees regarding deficiencies in the design or operation of Internal Controls and any fraud that involves management or other employees with a significant role in internal controls;

Operating staff

As aforementioned, all staff members should be responsible for reporting problems of operations, monitoring and improving their performance, and monitoring non-compliance with the corporate policies and various professional codes, or violations of policies, standards, practices and procedures. Internal Controls is all about continuous improvement of the Company policies and procedures, to enhance the overall efficiency and effectiveness of the organization itself. Staff and junior managers are involved in evaluating the controls within their own organizational unit, using a **control self-assessment**.

Limitations

Internal Controls can provide reasonable, not absolute, assurance that the objectives of an organization will be met. The concept of reasonable assurance implies a high degree of assurance, constrained by the costs and benefits of establishing incremental control procedures.

Effective internal control implies the organization generates reliable financial reporting and substantially complies with the laws and regulations that apply to it. However, effective internal control provides only timely information or feedback on progress towards the achievement of operational and strategic objectives, but cannot guarantee their achievement.

Internal controls for process improvement

Controls can be improved to make a business operation run more effectively and efficiently. Automating controls that are manual in nature can save costs, improving transaction processing. The Internal control system should not be thought only as a way of preventing fraud and complying with laws and regulations from the governance of the organization because an important opportunity may be missed. Internal controls can also be used to improve businesses, particularly in regard to effectiveness and efficiency.

Continuous controls monitoring

Advances in technology and data analysis have led to the development of numerous tools which can automatically evaluate the effectiveness of internal controls. Used in conjunction with continuous auditing, continuous controls monitoring provides assurance on financial information flowing through the business processes.

Fraud and internal control

Internal control plays an important role in the prevention and detection of fraud.[9] Under the Sarbanes-Oxley Act, companies are required to perform a fraud risk assessment and assess related controls.

2. The Sarbane Oaxley (SOX) act in the USA

The following paragraph is extracted from the PUBLIC LAW 107–204—JULY 30, 2002 of the 107th United States Congress:

> *"[…] **SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.***
>
> ***(a) RULES REQUIRED**.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—*
> *(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and*
> *(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.*
>
> ***(b) INTERNAL CONTROL EVALUATION AND REPORTING.**—With*
> *respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement. […]"*[5]

The Sarbane-Oaxley (SOX) Act, Section 404, is the law US corporations strive to comply with in terms of Internal Control structure. In order to better understand the mechanism that is involved in being compliant with the Act, we should analyze the parties playing key roles in this business, introducing some definitions.

Definitions

The **U.S. Securities and Exchange Commission** (**SEC**),
is an independent agency of the United States federal government. The SEC holds primary responsibility for enforcing the federal securities laws, proposing securities rules, and regulating the securities industry, the nation's stock and options exchanges, and other activities and organizations, including the electronic securities markets in the United States.[6]

The Securities Exchange Act of 1934 (Section 4) created the SEC, the Sarbanes–Oxley Act of 2002 then imposed the need for an Internal Control structure in public companies, and is commonly called SOX law.

The SEC has a three-part mission:

(a) protect investors;
(b) maintain fair, orderly, and efficient markets;
(c) facilitate capital formation.[7]

Fig.5 - SEC Logo

To achieve its mandate, the SEC enforces the statutory requirement that public companies and other regulated companies submit quarterly and annual reports, as well as other periodic reports. In addition to annual financial reports, company executives must provide a narrative account, called the "management discussion and analysis" (MD&A), that outlines the previous year of operations and explains how the company fared in that time period. MD&A will usually also touch on the upcoming year, outlining future goals and approaches to new projects. In an attempt to level the playing field for all investors, the SEC maintains an online database called EDGAR (the Electronic Data Gathering, Analysis, and Retrieval system) from which investors can access this and other information filed with the agency.

Quarterly and semiannual reports from public companies are crucial for investors to make sound decisions when investing in the capital markets. Unlike banking, investment in the capital markets is not guaranteed by the federal government. The potential for big gains needs to be weighed against that of sizable losses. Mandatory disclosure of financial and other information about the issuer and the security itself gives private individuals as well as large institutions the same basic facts about the public companies they invest in, thereby increasing public scrutiny while reducing insider trading and fraud.

The SEC makes reports available to the public through the EDGAR system. The SEC also offers publications on investment-related topics for public education. The same online system also takes tips and complaints from investors to help the SEC track down violators of the securities laws. The SEC adheres to a strict policy of never commenting on the existence or status of an ongoing investigation.

The **U.S. Public Company Accounting Oversight Board** (**PCAOB**), is a private, nonprofit corporation created by the Sarbanes–Oxley Act of 2002 to oversee the audits of public companies and other issuers in order to protect the interests of investors and further the public interest in the preparation of informative, accurate and independent audit reports. All PCAOB rules and standards must be approved by the U.S. Securities and Exchange Commission (SEC). In creating the PCAOB, the Sarbanes-Oxley Act mandated that auditors (external) of U.S. public companies must be subject to external and independent oversight, for the first time in history. Previously, the profession was self-regulated.

The PCAOB has four primary functions in overseeing auditors:

(a) registration of the auditors;
(b) inspection of audit reports;
(c) setting of the audit standards;
(d) enforcement in case of a finding.

Auditors of public companies are prohibited by the Sarbanes-Oxley Act to provide non-audit services, such as consulting, to their audit clients. This prohibition was made as a result of allegations, that auditors' independence from their clients had been compromised because of the large fees that audit firms were earning from such additional services.

PCAOB
Public Company Accounting Oversight Board

Fig.6 - PCAOB Logo

Powers of the PCAOB are subject to approval and oversight by the SEC. Individuals and audit firms subject to PCAOB oversight may appeal PCAOB decisions (including any disciplinary actions) to the SEC and the SEC has the power to modify or overturn PCAOB rules.

The PCAOB periodically Inspects registered public accounting firms. Reports are made public but portions of the inspection reports that treat potential defects in the audit quality are not made public if the firm addresses those matters to the PCAOB Board's satisfaction within 12 months from the report issuance date. Those portions are made public however, if the Board determines that a firm's efforts to address the criticisms or potential defects were not satisfactory, or the firm makes no submission evidencing any such efforts.[8]

The **SOX Compliance Program** of a US company is the planning and management of the whole structure that is implicitly created by SOX Act Sect. 404. This means that all the activities and frameworks that include SOX Financial Statement Controls and SOX Operational Controls are taken into account.

In particular these are:

(a) the Internal Controls Structure and Framework;
(b) the Self Assessment of the Controls;
(c) the SOX Internal Audit Testing (or Management Testing);
(d) the SOX External Audit Testing;
(e) the results Reporting to the Audit Committee;
(f) the Remediation plans.

All the activities related to these items require the deployment of a wide and well organized management structure, as well as the use and maintenance of tools for continuous controls monitoring. For wide spread organizations, all entities that are playing an important role in the consolidated financial statement creation, are taken into account regardless of the geographic and legal context where they operate. All the considerations about the Internal Controls Roles and Responsibilities are thus deployed to the organization's subsidiaries and business units in the world. This adds layers of complexity to the SOX Compliance Program requiring the Local Management, Operating Staff and Auditors to be aware of the objectives of the program, its timelines, testing procedures and evidences requested. Behavioral, Ethic and Cultural barriers need to be overcome in order to synchronize the whole machine and have it up and running.

The requirements and peculiarities of the aforementioned structure are such that a strong communication program must be performed, and a well defined and structured education program should be put in place starting from the "Tone at the Top" coming from Governance and Top Management of the organization.

The **Deficiencies in Internal Controls** are made public by the External Auditor (public audit firm) whenever a control is judged to be ineffective, after the discussion with the organization's management. Deficiencies are classified based on the underlying risk:

(a) **Control Deficiency** - A warning and request to perform better in the control activity, but nothing harmful to the organization;

(b) **Significant Deficiency** - A potential threat to the organization, that could lead to significant financial misstatements;

(c) **Material Weakness** - A serious risk of material financial misstatements for the organization.

The deficiencies can either be Aggregated or related to single Internal Controls. The outcome of a good SOX Compliance Program is a low number of deficiencies found and reported from the public auditor. Whenever an organization is raised exceptions such as Significant Deficiencies or Material Weaknesses, and these are made public, there normally is a decrease in the company's trust over Internal Controls and Financial Statements accuracy; thus the market and the organization's shares value is influenced by the situation.

In Deep

How are the described parties involved in assuring compliance to the SOX Act, satisfying SEC requirements, and being able to avoid, or remediate Control Deficiencies?

Every year the SOX Compliance Program is run. This means that every year the Controls are updated and improved, the evidences of the proper effectiveness of controls are collected and successively internally audited and then externally audited.
Internal testing (or Management testing) should be performed in the appropriate timeframe, such that (if performed from third party authorized auditing firms) the public auditor can eventually rely on the pre-existing testing results. Management's testing main aim is however to assess the effectiveness of controls and put remediation plans in place when needed, prior to the public auditor findings and pressures to remediate.

The SOX Compliance Program phases can be summarized in:

1. Internal Controls environment Update and Refresh;
2. Self Assessment of the Internal Controls;
3. Management Testing of the Internal Controls;
4. Public Auditors Testing of the Internal Controls;
5. Results and Reporting.

During the whole process described from points 1 to 5, the Internal Controls team is involved. In particular though, the Internal Controls team is involved in the first three phases and in the fifth one, as shown in the scheme reported in Fig.7.

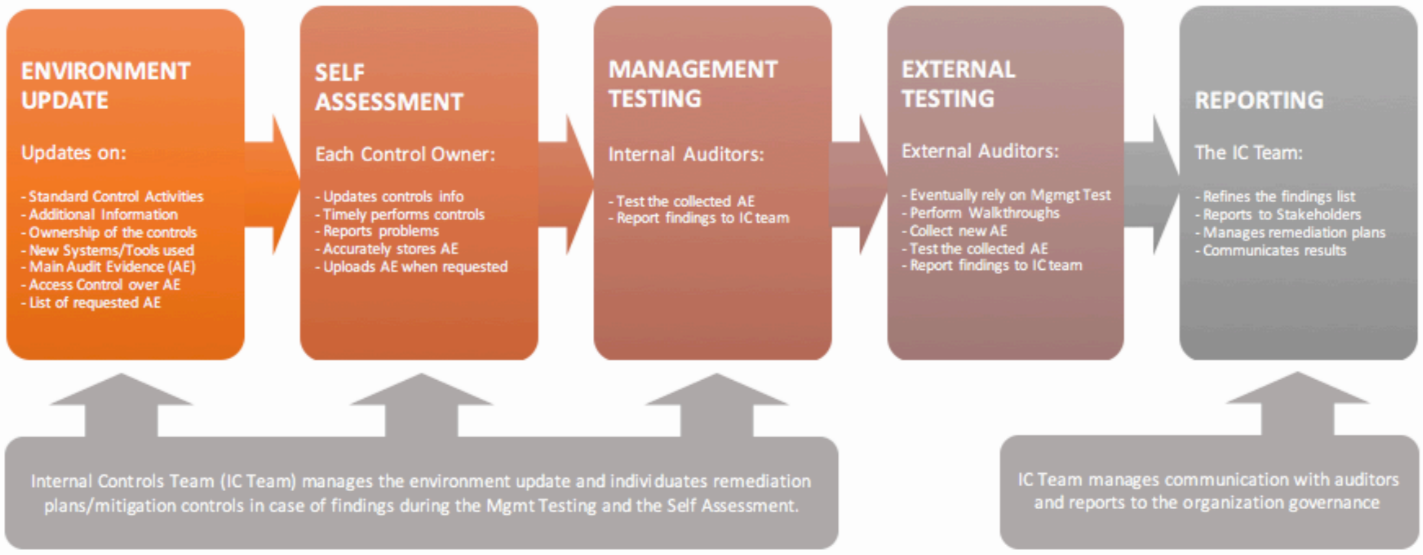


Fig.7 - The SOX Compliance Program recursive life cycle and the Internal Controls Team role.

3. SOX Internal Control environment within Bruker

This section's aim is to explain and illustrate how the COSO Internal Controls Framework and the Internal Controls Environment is maintained within Bruker. All the relevant parties and procedures/ methodologies used to manage the Internal Controls structure will be described.

Risks and Controls Matrices

Following COSO's best practices and procedures, Bruker Corporation performs risk management through setting an internal controls environment that is continuously updated and monitored. After a risk assessment phase, Risks and Controls Matrices are created and used as the knowledge base for the Internal Controls awareness and education within the Company.

A	C	E	F	K	L	M	N	O	P	R	S	T	V	W
Process Attributes			Risk Attributes	Financial Statement Assertions										
Business Cycle	Process	Control Objective	Risk	Classification	Cut-Off	EO	RO	CO	Transparency	VA	Accuracy	Risk Impact	Control Number	Standard Control Activity
OTC	Segregation of Duties - Cash Receipts	Duties are adequately segregated to prevent unauthorized or inappropriate entries from being processed and not detected.	When duties are not properly segregated, there is an increased risk that inappropriate or unauthorized activities may occur and not be detected.				X					Non-Key	OTC-01-01-01	Customer master file maintenance is restricted to a independent from goods & services issued, customer ir customer cash receipt processing and reconciliation ledger.
OTC	Segregation of Duties - Cash Receipts	Duties are adequately segregated to prevent unauthorized or inappropriate entries from being processed and not detected.	When duties are not properly segregated, there is an increased risk that inappropriate or unauthorized activities may occur and not be detected.				X					Non-Key	OTC-01-01-02	When customer master file maintenance is not restric users, system generated edit reports are independent appropriateness.
OTC	Segregation of Duties - Cash Receipts	Duties are adequately segregated to prevent unauthorized or inappropriate entries from being processed and not detected.	When duties are not properly segregated, there is an increased risk that inappropriate or unauthorized activities may occur and not be detected.				X					Key	OTC-01-01-03	The ability to prepare bank deposits and record cash r segregated from the bank account reconciliatio
OTC	Segregation of Duties - Cash Receipts	Duties are adequately segregated to prevent unauthorized or inappropriate entries from being processed and not detected.	When duties are not properly segregated, there is an increased risk that inappropriate or unauthorized activities may occur and not be detected.				X					Non-Key	OTC-01-01-04	Access to control cash receipt programs in the syster authorized users independent from customer master f customer invoice processing and customer receipt proc
OTC	Contract Review	Customer contracts are valid.	Unauthorized, incomplete or inaccurate terms and conditions are agreed with customers increasing the risk of unfavorable terms or adverse financial impact.				X					Key	OTC-02-01-01	Customer contracts are reviewed and approved in acc Contracts Signature Authorization Mat

Fig.8 - RCM Example, Risk and Control Objectives are reported then Standard Control Activities are developed and shared across the organization.

Before my internship at Bruker a long and complex process of global realignment on platforms, methods and procedures was initiated. This also touched Internal Controls that started "rationalizing" all the legal entities, promoting and sponsoring a Global Set of well crafted controls tailored to the specifications of the Committee of Sponsoring Organizations of the Treadway Commission Framework. This is leading legal entities within Bruker's organization to have a Risks and Controls Matrix, describing the activities that local management and operational staff perform in order to satisfy the control requirements and the Sarbane-Oaxley Act. Before such global set of "standard controls" was put in place, almost every entity had its own set of "legacy controls", full of weaknesses in important areas while having redundant operational internal controls that were not in the SOX testing scope due to low financial misstatement risk.

The operation of the sponsoring and promoting of the Global Controls framework is really meant to facilitate the work of the legal entities of the organization. However sometimes due to Ethical, Cultural and Behavior based barriers it is difficult to let the local involved personnel understand the importance of having a globally shared unique structure. This limits the individual flexibility on the task completion but enables a complete different scenario for the continuous update, management and monitoring of the system.

It is important to know that the Internal Controls team at Bruker was on development at the time of the internship. In-fact in order to manage/monitor approximately 900 controls across 22 different business units all over the world, a total headcount of 3 persons also considering interns was allocated.

Fig.9 - Part of the RCM reserved to responsibilities.

Control Owners/Reviewers/Preparers

The convenience of using a standard framework to identify the Internal Controls that defines policies, procedures and risk coverage has already been illustrated. Although this seems fairly understandable, there still is a need to perform change management and training efforts to spread the awareness in the organization, to make sure the advantages are recognized within whole Bruker. A classification of users and their roles and responsibilities is part of the educational program about SOX Compliance, and the Risks and Controls Matrix tries to frame and capture this information. In particular, the SOX team defined the roles of:

(a) **Control Owners:** are those who are responsible for the Controls operative effectiveness, and are supplying evidence/reviewing work and maintaining the additional information requested every year on updates/changes to the control;

(b) **Control Reviewers:** those persons that Review and properly submit evidence of review in case of review type controls (controls that involve a Management judgement on some information). In the review type controls case, Reviewers are also Owners of the control. In non-review type controls (authorization controls) they just supervise the work of the Control Preparers and authorize actions where needed;

(c) **Control Preparers:** are the persons entitled to the operational part of the control. Control Preparers elaborate the information on the basis of which the control is evaluated, be it a review type control or an authorization type control. Control Preparers can also be Control Owners but they CAN'T BE Reviewers for Segregation of Duties purposes.

The Controls Refresh Program

The Controls Refresh Program is the media used by Bruker to update/change/revise the Internal Controls structure knowledge base every year. In order to perform this task, every Control Owner is asked if there are changes in the controls they own and to update additional information to their controls status and operation effectiveness. This is part of the "Self Assessment" that should be performed by every Control Owner on behalf of the organization.

Remembering Bruker organizational structure complexity and the need of managing 900 controls over 21 different countries, it is well evident how processes like the Refresh Program should be centrally managed but locally performed. Without this top-down way of performing the operations on SOX controls, it would be nearly impossible for a central SOX Team to drive the Compliance program and enhance business performances and controls reliability. The Risks and Controls Matrix of every location is updated during the Refresh Program.

Internal Auditors

In order to perform the Management testing due to available resources and the prohibitive dimension of the structure, and also to maximize the reliance model on management testing from the public auditor, an external Auditing Firm is hired by Bruker.

Auditors from all over the world partnering with the hired audit firm audit the internal controls at various location.

External Auditors

As for many large public companies, the hired public auditor is usually one of the big 4 audit firms. For the Fiscal Year 2016, Bruker's client in auditing the Internal Controls structure was PriceWaterhouseCoopers (PWC).

Prepared By Client (PBC) lists

Whenever Internal Controls should be audited (Management testing or External testing), audit evidences have to be requested to the right personnel in the organization (Controls Owners), collected and stored centrally from the SOX Team (only for Internal Audit) to facilitate the audit procedures creating efficiencies. In order to do so, for each audit the SOX Team in collaboration with the Client (in this case the Internal Auditors) develops a "per-control" list of evidences that should be collected from Control Owners for the testing to be performed. This list is called Prepared By Client list. External Auditors have their own PBC List and collect the information on their own, eventually relying on some of the evidences and testing procedures of the Management testing.

Control Description	Additional Information	Category	Period Requested	Request	Attachment
Revenue recognition checklists or memos are prepared by Finance for significant/complex orders and are reviewed and approved in accordance with the Revenue Recognition Policy.	All entities are required to submit each month a one page Revenue Recognition Checklist ("RRC") for all third-party product sales $1M or greater or their highest product sale in the month. The RRC summarizes the terms and conditions of the sale, how much has been recognized in the month and any remaining deliverables. The RRC's are prepared by the local entity and then submitted to Corporate Accounting for review.	B	March and April 2017	1) "Provide the Revenue Recognition Checklists ("RRC") for listed month, from these checklists, we will make a sample selection to complete testwork.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
		B		2) Provide the monthly summary of RRC review and findings with evidence of review by the VP of Finance and CAO.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
The company has established a world-wide Revenue Recognition Policy.	This policy is available on sharepoint and is reviewed annually by the Director of Technical Accounting. As part of the revenue recognition policy is a Revenue Recognition matrix which documents the Company's products into A,B,C categories and guides revenue recognition criteria. This matrix is updated on a quarterly basis with each Division. Starting in Q2 2016, the matrix is also starting to capture for certain systems the fair value of other deliverables in an order (installation, maintenance, training) when sold as part of a multiple-element arrangement.	B	Annual	1) Provide the latest version of the company's Revenue Recognition Policy.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
The External Reporting Manager or designee summarizes all acceptance documentation received after quarter-end but relates to the current quarter in which revenue should have been recognized. An estimated COGS amount is applied to the revenue to determine an estimated gross profit amount that would have been recognized. If the estimated gross profit amount is considered material to the quarter, then an adjusting entry is recorded in the current quarter. The summary of findings is documented in the Revenue memo and reviewed by the Assistant Corporate Controller or CAO.	The Director of Technical Accounting (Scott Sewall) reviews the acceptance documentation after the quarter close	B	Q1 2017	1) Provide summary findings documented in the revenue memo for quarter requested. We will verify the memo has been reviewed by the Assistant Corporate Controller or CAO.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
Customer-facing personnel must certify quarterly that no side agreements exist; no letters of commitments or verbal agreements that modify or amend terms of customer contracts exist; and no billable services have been provided free of charge. Finance reviews and documents the results of the certifications in the quarterly revenue recognition memo.	No updates deemed necessary	A	Q1 2017	1) Provide Q1 2017 quarterly lists of all Sales personnel that are required to provide a sales certification.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
		B		2) We will select a sample of individuals to test, please make certification available.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
		B		3) Please provide reviewed quarterly revenue recognition memos.	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.

Fig.10 - PBC List Example, all the evidence requested for testing are reported per control.

Issues List

When a management testing is performed Internal Auditors either confirm the effectiveness of the controls or provide some Findings and Recommendations to remediate the ineffective controls. In Bruker for the ineffective controls and their related findings, a "Issues List" is created.
The issues list needs to be reviewed from the SOX Team for every location and subsequently approved by local management prior to be included in the Management Testing Summary of Control Deficiencies (SOCD) list. External Auditors prepare a SOCD list too, refining the list on their own and submitting a final revision to the SOX Team that will be further discussed.

Summary of Controls Deficiencies list

The Internal Summary of Controls Deficiencies list in Bruker is further refined from the SOX Team and then submitted to the Audit Committee both for Internal Audit and External Audit. Every refinement of the list needs to be discussed with the related auditors prior to edits/changes.

Side Note

All the mentioned structure about Bruker SOX Compliance Program requires management tools and procedures. The aforementioned program was managed manually before my internship (through emails, or through Excel files exchanged on the Company's intranet).

I was hired as a "Systems Engineering Expert" Intern to Manage the hired Consultancy firm that was customizing the chosen software platform to drive the SOX Compliance Program for the FY 2016. As it can be proved from an analysis of my Performance Goals set for the internship, my role was to provide both technical and business oriented guidance and management over the development of Bruker's "Wdesk platform". The latter was created to perform the Refresh

Program, the Communication with Control Owners and stakeholders, the central collection and storage of Controls Evidences, the SOX Controls Audit and results Reporting.

My work was positively commented from Senior Management and this provided exposure to business partners and Bruker's governance team, to the point that I was included in special financial initiatives and business operations (see "Inside The Business" section).

The engineering knowledge gained through the MSc course at Polytechnic University of Turin was of outstanding importance to complete the tasks I was assigned to, and to be included in top financial management experiences which hugely impacted my understanding of business, improving my skills set. Considering the whole SOX Compliance Program as a system to keep Bruker Company under control as far as Financial health and laws/regulatory compliance, it is possible to find analogies with the widely studied models during Controls Systems courses at PoliTO. The SOX Program is just a feedback control over the Internal Control Environment, that updates the information based on the previous year outcomes and makes it possible to track the reference of a zero deficiencies Internal Controls Environment as ideally required by the SOX law (Fig.11).

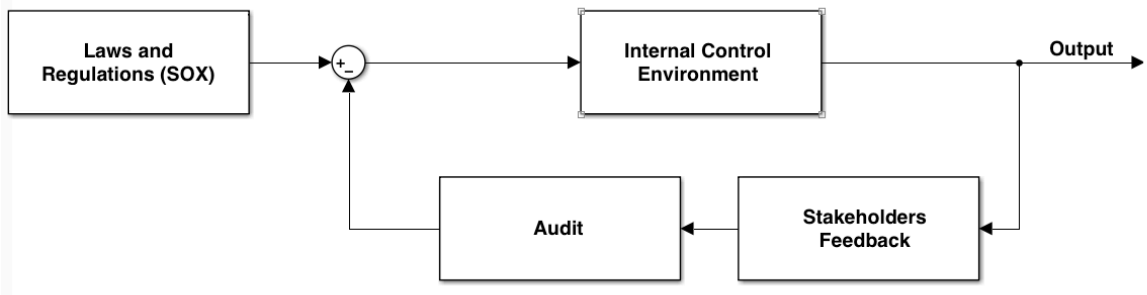


Fig.11 - Representing the SOX Compliance Program as a feedback control system.

(3) Tools and Instruments used

1. Microsoft Project

Microsoft Project is a project management software product, developed and sold by Microsoft. It is designed to assist a project manager in developing a plan, assigning resources to tasks, tracking progress, managing the budget, and analyzing workloads. Within a couple of years from its introduction in 1984 it became the dominant PC-based project management software.[10]
Microsoft Project and Microsoft Project Server are the cornerstones of the Microsoft Office enterprise project management (EPM) product.

Fig.12 - Microsoft Project logo.

Project creates budgets based on assignment work and resource rates. As resources are assigned to tasks and assignment work estimated, the program calculates the cost, equal to the work times the rate, which rolls up to the task level and then to any summary tasks and finally to the project level. Each resource can have its own calendar, resource rates are used to calculate resource assignment costs which are rolled up and summarized at the resource and project level. Microsoft Project is unsuitable for solving problems of available materials constrained production, but it is appropriate for work resources management.
The application creates critical path schedules, and critical chain and event chain methodology.

Schedules can be resource leveled, and chains are visualized in a Gantt chart. Custom objects such as calendars, views, tables, filters, and fields are stored in an enterprise global which is shared by all users.

2. Workiva Wdesk

Workiva is an enterprise software company based in Ames, Iowa. Founded in 2008 as Webfilings, its main product is Wdesk, a cloud-based enterprise management and auditing software-as-a-service platform that enables companies to create and file financial and compliance reports and documents to the SEC. Wdesk platform integrates information including spreadsheets, presentation documents, and other unstructured data, into a single cloud-based report.[11][12] The company employs approximately 1,200 people with offices in 16 cities in the United States, Canada and Europe.[11]

Workiva first SaaS product was SEC reporting software that enabled companies to file electronically directly with the SEC, using the business mark-up language XBRL (Extensible Business Reporting Language), required by the SEC.[13] A Workiva customer was the first company to file Inline XBRL with the SEC.[14]

Fig.13 - Workiva Wdesk logo.

The company has since expanded to include other corporate financial and compliance reporting functions, including: SOX reporting, Recovery and Resolution Plans (RRP). WDesk integrates documentation required for financial statements, risk assessment and forecasts required by the Sarbanes-Oxley Act into a single view, as well as bundled audit features.[15]

In 2016, Forbes magazine recognized Workiva as one of the 25 Highest-Rated Public Cloud Computing Companies To Work For.[16]
Workiva ranked #4 on Fortune magazine's 2016 Top 10 Best Large Workplaces in Technology[17] and ranked #6 on Fortune magazine's Top 50 Best Large Workplaces.

3. Microsoft SharePoint

SharePoint is a web-based, collaborative platform that integrates with Microsoft Office, launched in 2001.[18] Microsoft states that SharePoint has 190 million users across 200,000 customer organizations.[19]

SharePoint allows for storage, retrieval, searching, archiving, tracking, management, and reporting on of electronic documents and records.[20] SharePoint's integration with Microsoft Windows and Microsoft Office allow for collaborative real-time editing, and encrypted/information rights managed synchronization.

Fig.14 - Microsoft SharePoint logo.

A SharePoint intranet or portal is a way to centralize access to enterprise information and applications. It is a tool that helps an organization manage its internal communications, applications and information more easily. Microsoft claims that this has organizational benefits such as increased employee engagement, centralizing process management, reducing new staff on-boarding costs, and providing the means to capture and share tacit knowledge (via tools such as wikis).

SharePoint contains team collaboration groupware capabilities, including: Project scheduling (integrated with Outlook and Project), social collaboration, and project related document storage and collaboration. Groupware in SharePoint is based around the concept of a "Team Site".

Examples of Site templates in SharePoint include: collaboration (team) sites, wiki sites, blank sites, and publishing sites.

4. Ipswitch iMacros

Ipswitch is an IT management software developer for small and medium sized businesses.[21] The company was founded in 1991 and is headquartered in Lexington, Massachusetts.

In 2008, Ipswitch split its operations into three divisions, secure file transfers, network management, and messaging and collaboration. In December 2012, Ipswitch acquired the Waldorf, Germany-based performance testing company iOpus known for its product, iMacros, a web-browser extension.[22]

Fig.15 - Ipswitch iMacros logo.

iMacros is an extension for the Mozilla Firefox, Google Chrome, and Internet Explorer web browsers, developed by iOpus/Ipswitch. The macros can be combined and controlled via JavaScript. Along with the freeware version, iMacros is available as a proprietary commercial application,[23] with additional features and support for web scripting, web scraping, internet server monitoring, and web testing. In addition to working with HTML pages, the commercial editions can automate Adobe Flash, Adobe Flex, Silverlight, and Java applets by using Directscreen and image recognition technology. Advanced versions also contain a command-line interface and an application programming interface (API) to automate more complicated tasks and integrate with other programs or scripts. The iMacros API is called the Scripting Interface. The Scripting Interface of the iMacros Scripting Edition is designed as a Component Object Model (COM) object and allows the user to remotely control the iMacros Browser, Internet Explorer, Firefox and Chrome from any Windows programming or scripting language.[24]

(4) Thesis structure

1. Further sections brief description

After the proper introduction, setting the ground for the reader to understand operations that were carried out during the internship, the thesis is divided in 4 further sections:

1. Execution; 2. Inside the Business; 3. Conclusions; 4. Thanks

Let's tear down what is going to be described in these sections.

1. Execution

This part of the document is describing the operations carried out during the whole internship:

- SOX Program restructuring
- SOX Program communication
- Data acquirement
- Project management
- Audit planning & execution
- Results collection & communication

The section also includes the structure of the SOX Program inside Bruker Corporation, and how the program was run in year 2016 by the corporation.

2. Inside the Business

This part of the document is reserved to two particular events occurred during the internship:

- Bruker Nano Berlin rationalization
- Global SAP Access Review control remediation

The concept of rationalization is explained, together with Bruker Nano Berlin entity presentation. Regarding the Global SAP Access Review control, the failing approach used in 2015 is described and the development of a new approach based on Robotic Process Automation software, that was put in place by the candidate in 2016, is analyzed in deep.

3. Conclusions

The conclusions section reports some thoughts of the candidate on the fusion of a very technical profile such as that of an Engineer with the tasks and skills of the Management roles.

4. Thanks

The thanks section is reserved to the personal thanks of the candidate to those whose effort made the realization of this document possible.

III. Execution

(1) Management of the SOX Program

1. Workiva Wdesk for Bruker SOX Compliance Program

For FY2016, Internal Controls Snr. Management decided to implement the software platform "Workiva Wdesk" with the intention of integrating:

(a) The Refresh Program;

(b) The distribution of PBC Lists;

(c) Electronic Audit Evidences collection;

(d) Audit procedures for Management Testing.

The whole SOX Compliance Program was migrated into Wdesk platform. Since the program was handled through Excel files before which are a very flexible business standard, it kept the same format within Wdesk although enabling the possibility of "linking" spreadsheets.

The use of Wdesk introduced the need of diverse and significant efforts to define:

I. Documents structure development and management;

II. A Permissions/Security framework;

III. Users & Accounts management;

The documents structure really is the same described in section "5 - SOX Internal Control environment within Bruker". The most thrilling part of the structure definition was the creation of relations among the spreadsheets that defined the "Links" which were actually creating efficiency across the whole program. This way the performances analysis and the audit results collection were easy and immediate.

Wdesk works in a very similar way to a DBMS, with the difference that in a Data Base Management System the relations are defined and then cannot be modified from the Application that is built upon the Data Base.

On the contrary, Wdesk enables the possibility to target cells and columns, linking them to other spreadsheets creating a "live" platform that can always be modified while being used. The structure represented in Fig.16 was defined and successively built with the help of Workiva consultants.

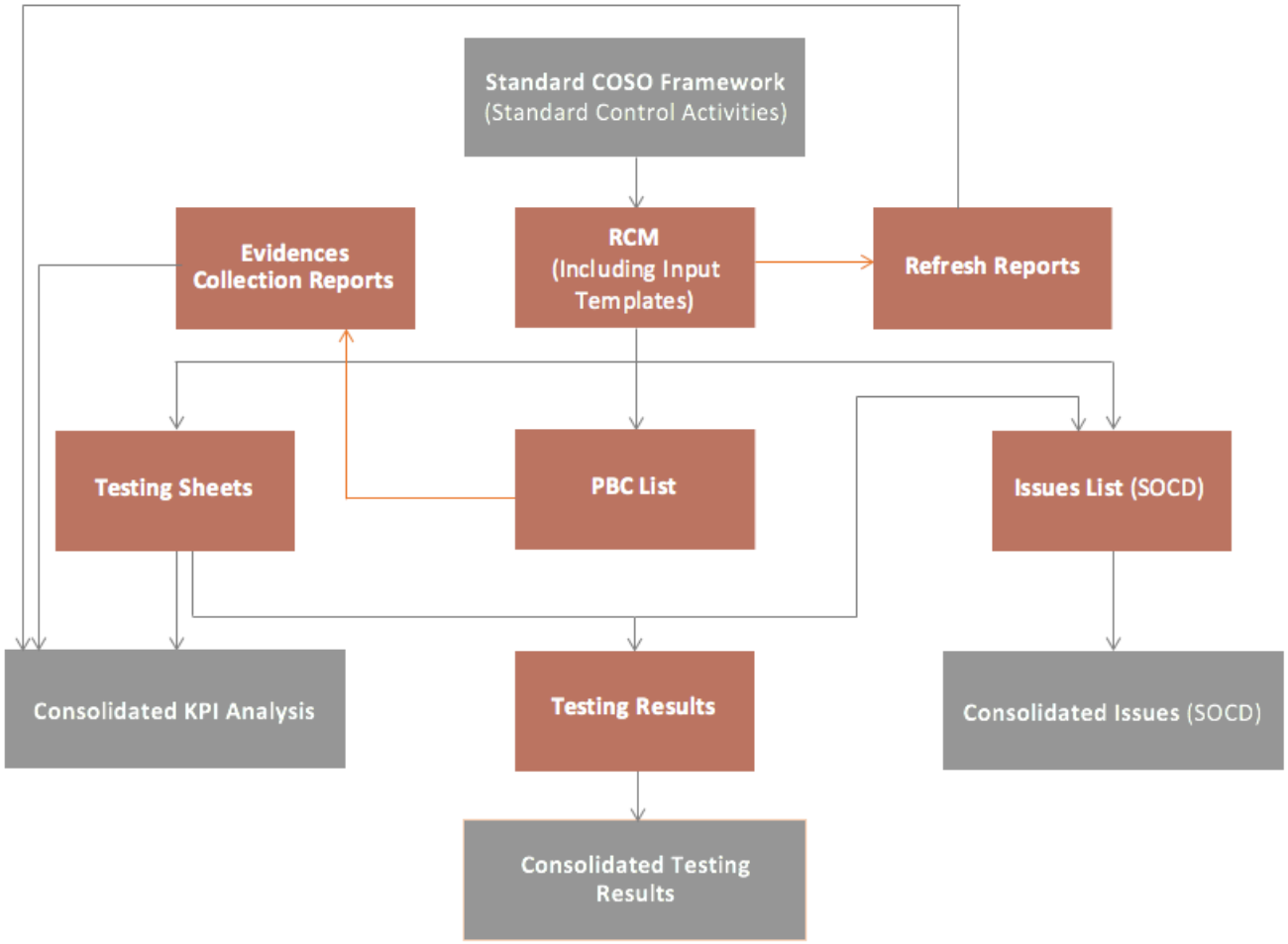


Fig.16 - Bruker Wdesk SOX Compliance program spreadsheet relations. Orange: Entity related; Grey: Consolidated.

Using the above structure, whenever a Control Owner provided input (through specifically targeted Input Templates) the information flew inside a series of linked spreadsheet such as: Testing Sheets, Test tracking matrices, PBC Lists, SOCDs, etc.

In Deep

Let's describe each document reported in Fig.16, and its interconnection with other documents among the platform (only forward linking reported):

The **Standard COSO Framework** document, is a mapping spreadsheet consisting of a table that contains Control Objectives, Associated Risks, Standard Controls Language, Assertion properties for the controls and other useful information referred to the Standard Control activities. The set of mapping tables and information is sponsored from PWC public auditor, and comes from the result of a study concerning risk assessment of public companies in the United States.

Links:

Linked to: *Risks and Controls Matrixes* by means of:

- Standard Control Activity
- Control ID
- Standard Risk Objective
- Standard Control Assertions

The **Risks and Controls Matrix (RCM)** documents, belong to each controlled legal entity (one matrix for one entity) and consist of all the controls Standard Language coming from the Standard COSO Framework document, and the additional information provided by Control Owners concerning the specific Control Activity. These files include the "Input Templates" that will further be discussed later, and consist in a series of questions asked to the Control Owner in order to determine information about the control during the Refresh Program. These spreadsheets are used from Internal Auditor, External Auditor and IC Team to either test or discuss control activities.

Links:

Linked to: *PBC List* documents by means of:

- Standard Control Activity
- Control ID
- Additional Information
- Control Owner

Linked to: Refresh Reports documents by means of:

- Completed Input Templates
- Control ID
- Control Owner

Linked to: Testing Sheets documents by means of:

- Standard Control Activity
- Control ID
- Additional Information
- Control Owner

Linked to: Issues List documents by means of:

- Standard Control Activity
- Control ID
- Additional Information
- Control Owner

The **Refresh Report** documents, belong to each controlled legal entity (one report for one entity) and consist of a measure of the number of Input Templates filled by the Control Owners. The information is coming from the RCM of each entity, thanks to a cell which status is changed automatically when all the questions are answered (Completed Input Template).

Links:

Linked to: *Consolidated KPI analysis* document by means of:

- Completed Input Template
- Control ID
- Entity ID
- Control Owner

The **PBC List** documents, belong to each controlled legal entity (one list for one entity) and consist of a list of Audit Evidence to be uploaded, requested to the Control Owners. The list mentioned here is the Management Testing list. Each control (information coming from the RCM) generates one or more audit evidence request (e.g. “Upload Billing Due List report”).

Links:

Linked to: *Evidences Collection Report* document by means of:

- Completed Request
- Control ID
- Control Owner

The **Evidences Collection Report** documents, belong to each controlled legal entity (one report for one entity) and consist of a measure of the number of requests fulfilled by the Control Owners. The information is coming from PBC List of each entity, thanks to a cell which status is changed by the Control Owner when he/she performs the requested action (e.g. "File Attached: Upload Billing Due List report").

Links:

Linked to: *Consolidated KPI analysis* document by means of:

- Completed Request
- Control ID
- Entity ID
- Control Owner

The **Testing Sheets** documents, belong to each controlled legal entity (one document for one entity) and consist of a group of procedures/testing spreadsheets, one for each control that needs to be tested in each entity. The information is coming from the RCM of each entity, Internal Auditors use these Testing Sheets to validate the controls operating effectiveness and sign-off on these documents after the audit review.

Links:

Linked to: *Testing Results* document by means of:

- Control Operating Effectiveness
- Finding
- Notes
- Control ID
- Control Owner

Linked to: *Issues List* document by means of:

- Control Operating Effectiveness
- Finding
- Notes
- Control ID
- Control Owner

Linked to: *Consolidated KPI analysis* document by means of:

- Entity ID
- Control Operating Effectiveness

The **Issues List** documents, belong to each controlled legal entity (one list for one entity) and consist of a description of all the findings and notes in the entity controls judged ineffective by the Internal Auditors. Also called *"Local Summary of Controls Deficiencies (LSOCD)",* the information is coming from the RCM and the Testing Sheets of each entity and it is mainly used to set action plans to remediate controls deficiencies.

Links:

Linked to: *Consolidated Issues* document by means of:

- Control Operating Effectiveness
- Control ID
- Finding
- Notes
- Entity ID

The **Testing Results** documents, belong to each controlled legal entity (one result file for one entity) and consist of a dashboard to properly visualize and discuss testing results of the entity. The information is coming from the Testing Sheets of each entity, it includes the detail of findings and notes of the failing controls but is intended to discuss results and not to set action items.

Links:

Linked to: *Consolidated Testing Results* document by means of:

- Control Operating Effectiveness
- Control ID
- Entity ID

The **Consolidated KPI Analysis** document parametrizes the whole system and enables the possibility of a comparison in time of the Key Performance Indicators of the program. Information is coming from Testing Sheets, Evidence collection reports, Refresh reports. The main monitored KPIs for FY2016 were: Overall refresh program completion, Overall evidences collection completion, Deadlines in refresh program met, Deadlines in evidences collection met, Overall Ineffective controls number, Controls deficiencies per Business Cycle (OTC, PTP, INV, etc.). These KPIs were introduced by the candidate and judged meaningful thus monitored by the management of the company.

The **Consolidated Issues (SOCD)** document shows all the Ineffective controls globally and the related action plans for deficiencies remediation status. Information is coming from Issues Lists of all the entities. The main aim is to properly track remediation plans without entering in the detail, that can be found in local SOCD List.

The **Consolidated Testing Results** document shows the results of controls testing globally, in a graphical and simplified view. Information is coming from Testing Results of all the entities. The main aim is to show the performance of Internal Controls in the year, presenting it to stakeholders and Top Management of the corporation.

2. Sharepoint wiki website - Wdesk Support website

As the COSO Internal Control Framework specifies (see Fig.4, page8), Information & Communication is a core activity of the Internal Controls structure that also enables the possibility of Control Owners to carry out their control work respecting their responsibilities. During my internship I came up with the idea of realizing a Sharepoint Wiki website, trying to leverage a tool (MS SharePoint) that Bruker corporation is successfully using in other ways (storing of models, documentation, projects).

The main important items that the stakeholders (Control Owners, General Managers and Business Leaders of the organization) struggled to find in previous years editions of the SOX Compliance Program were:

1. Understanding of their responsibilities;
2. Status of the Program;
3. Performances measurement over the Refresh Program;
4. Timeline of the whole SOX Compliance Program.

This fact led the SOX "WDESK SUPPORT" wiki website development project, that comprehended the following sections:

I. Home Page
II. Users Type Table
III. Technical Support
IV. Content Support

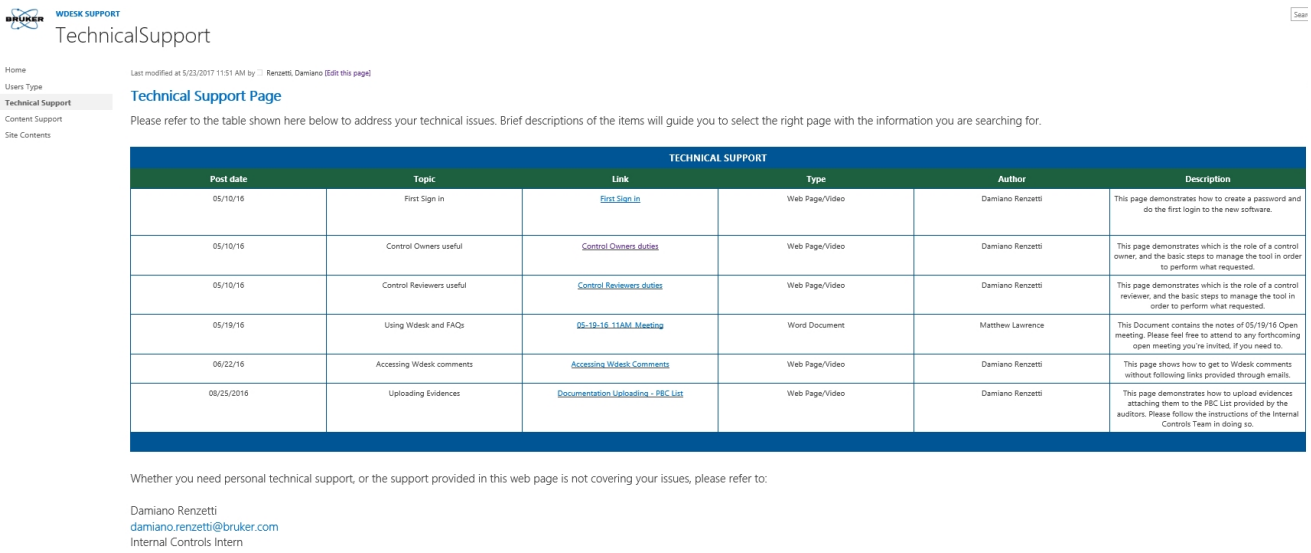
Examples are reported in figures Fig.18 and Fig.19. However, the

Home Page offered a glance on last updates regarding the Audit Plan and the Refresh Program phases on Wdesk platform;

Users Type Table defined users and the actions they were supposed to perform in Wdesk, in what time and for which reason;

Technical Support contained videos of operations the stakeholders had to perform on the platform as shown in Chapter 10 of this document;

Content Support included knowledge on financial controls and the Internal Controls duties in general for Control Owners.



WDESK SUPPORT

TechnicalSupport

Home
Users Type
Technical Support
Content Support
Site Contents

Last modified at 5/23/2017 11:51 AM by Renzetti, Damiano [Edit this page]

Technical Support Page

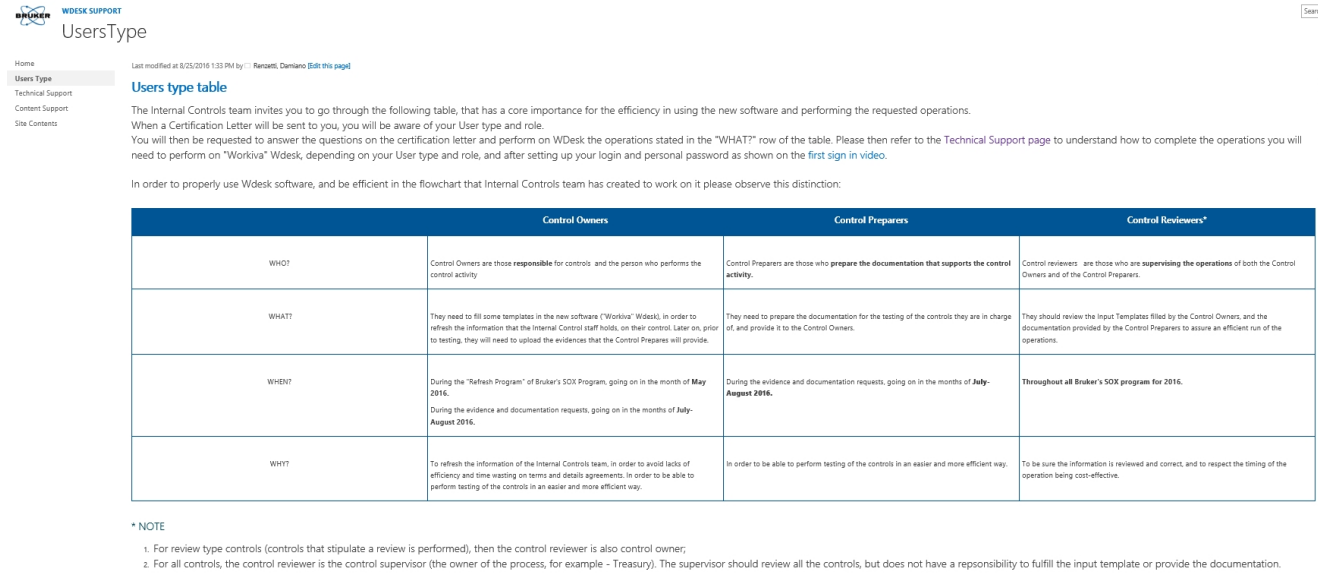
Please refer to the table shown here below to address your technical issues. Brief descriptions of the items will guide you to select the right page with the information you are searching for.

TECHNICAL SUPPORT					
Post date	**Topic**	**Link**	**Type**	**Author**	**Description**
05/10/16	First Sign in	First Sign in	Web Page/Video	Damiano Renzetti	This page demonstrates how to create a password and do the first login to the new software.
05/10/16	Control Owners useful	Control Owners duties	Web Page/Video	Damiano Renzetti	This page demonstrates which is the role of a control owner, and the basic steps to manage the tool in order to perform what requested.
05/10/16	Control Reviewers useful	Control Reviewers duties	Web Page/Video	Damiano Renzetti	This page demonstrates which is the role of a control reviewer, and the basic steps to manage the tool in order to perform what requested.
05/19/16	Using Wdesk and FAQs	05-19-16_11AM_Meeting	Word Document	Matthew Lawrence	This Document contains the notes of 05/19/16 Open meeting. Please feel free to attend to any forthcoming open meeting you're invited, if you need to.
06/22/16	Accessing Wdesk comments	Accessing Wdesk Comments	Web Page/Video	Damiano Renzetti	This page shows how to get to Wdesk comments without following links provided through emails.
08/25/2016	Uploading Evidences	Documentation Uploading - PBC List	Web Page/Video	Damiano Renzetti	This page demonstrates how to upload evidences attaching them to the PBC List provided by the auditors. Please follow the instructions of the Internal Controls Team in doing so.

Whether you need personal technical support, or the support provided in this web page is not covering your issues, please refer to:

Damiano Renzetti
damiano.renzetti@bruker.com
Internal Controls Intern

Fig.18 - SharePoint Wiki website - Technical Support Page.



WDESK SUPPORT

UsersType

Home
Users Type
Technical Support
Content Support
Site Contents

Last modified at 8/25/2016 1:33 PM by Renzetti, Damiano [Edit this page]

Users type table

The Internal Controls team invites you to go through the following table, that has a core importance for the efficiency in using the new software and performing the requested operations.
When a Certification Letter will be sent to you, you will be aware of your User type and role.
You will then be requested to answer the questions on the certification letter and perform on WDesk the operations stated in the "WHAT?" row of the table. Please then refer to the Technical Support page to understand how to complete the operations you will need to perform on "Workiva" Wdesk, depending on your User type and role, and after setting up your login and personal password as shown on the first sign in video.

In order to properly use Wdesk software, and be efficient in the flowchart that Internal Controls team has created to work on it please observe this distinction:

	Control Owners	**Control Preparers**	**Control Reviewers***
WHO?	Control Owners are those **responsible** for controls and the person who performs the control activity	Control Preparers are those who **prepare the documentation that supports the control activity.**	Control reviewers are those who are **supervising the operations** of both the Control Owners and of the Control Preparers.
WHAT?	They need to fill some templates in the new software ("Workiva" Wdesk), in order to refresh the information that the Internal Control staff holds, on their control. Later on, prior to testing, they will need to upload the evidences that the Control Prepares will provide.	They need to prepare the documentation for the testing of the controls they are in charge of, and provide it to the Control Owners.	They should review the Input Templates filled by the Control Owners, and the documentation provided by the Control Preparers to assure an efficient run of the operations.
WHEN?	During the "Refresh Program" of Bruker's SOX Program, going on in the month of **May 2016.** During the evidence and documentation requests, going on in the months of **July-August 2016.**	During the evidence and documentation requests, going on in the months of **July-August 2016.**	**Throughout all Bruker's SOX program for 2016.**
WHY?	To refresh the information of the Internal Controls team, in order to avoid lacks of efficiency and time wasting on terms and details agreements. In order to be able to perform testing of the controls in an easier and more efficient way.	In order to be able to perform testing of the controls in an easier and more efficient way.	To be sure the information is reviewed and correct, and to respect the timing of the operation being cost-effective.

* NOTE

1. For review type controls (controls that stipulate a review is performed), then the control reviewer is also control owner;
2. For all controls, the control reviewer is the control supervisor (the owner of the process, for example - Treasury). The supervisor should review all the controls, but does not have a repsonsibility to fulfill the input template or provide the documentation.

Fig.19 - SharePoint Wiki website - Users Type Table.

For change management purposes, during the whole year communications about the new platform and the roles and responsibilities of personnel involved with the SOX Program were sent out via emails, and notified to interested individuals. Although the use of emails and targeted communications/meetings is effective within the environment, the most useful and productive media for sharing knowledge is nowadays represented by videos.

During the internship I had the idea of realizing walk-through videos to describe step-by-step operations that stakeholders had to perform on Wdesk platform. The videos along with text explanations were hosted on the same Sharepoint wiki website that proved to be very useful and a great communication tool.

Fig.17 - Example of a training video created and hosted on the SharePoint Wiki website.

3. Refresh Program - Risks and Controls Matrices

As discussed, Risk and Controls Matrices are used for the description and definition of Internal Controls within each in-scope entity. Let's analyze them in-deep and understand which fields needs to be updated from the Control Owners during the Refresh Program, and how it was made possible for them to update such information.

Control Number	Standard Control Activity	Additional Information	Electronic Audit Evidence ("EAE"): Key Reports / Spreadsheets	Frequency	Control Activity Owner	Preparer	Control Reviewer	Define "Review" performed	How does control owner ensure that the underlying support/analysis is accurate and complete?	How is review evidenced?	Access Controls for EAE

Fig.20 - Control information to be updated from Control Owner in RCM.

The white cells in Fig.20 represent the fields that should be continuously updated by the Control Owners of the Company.

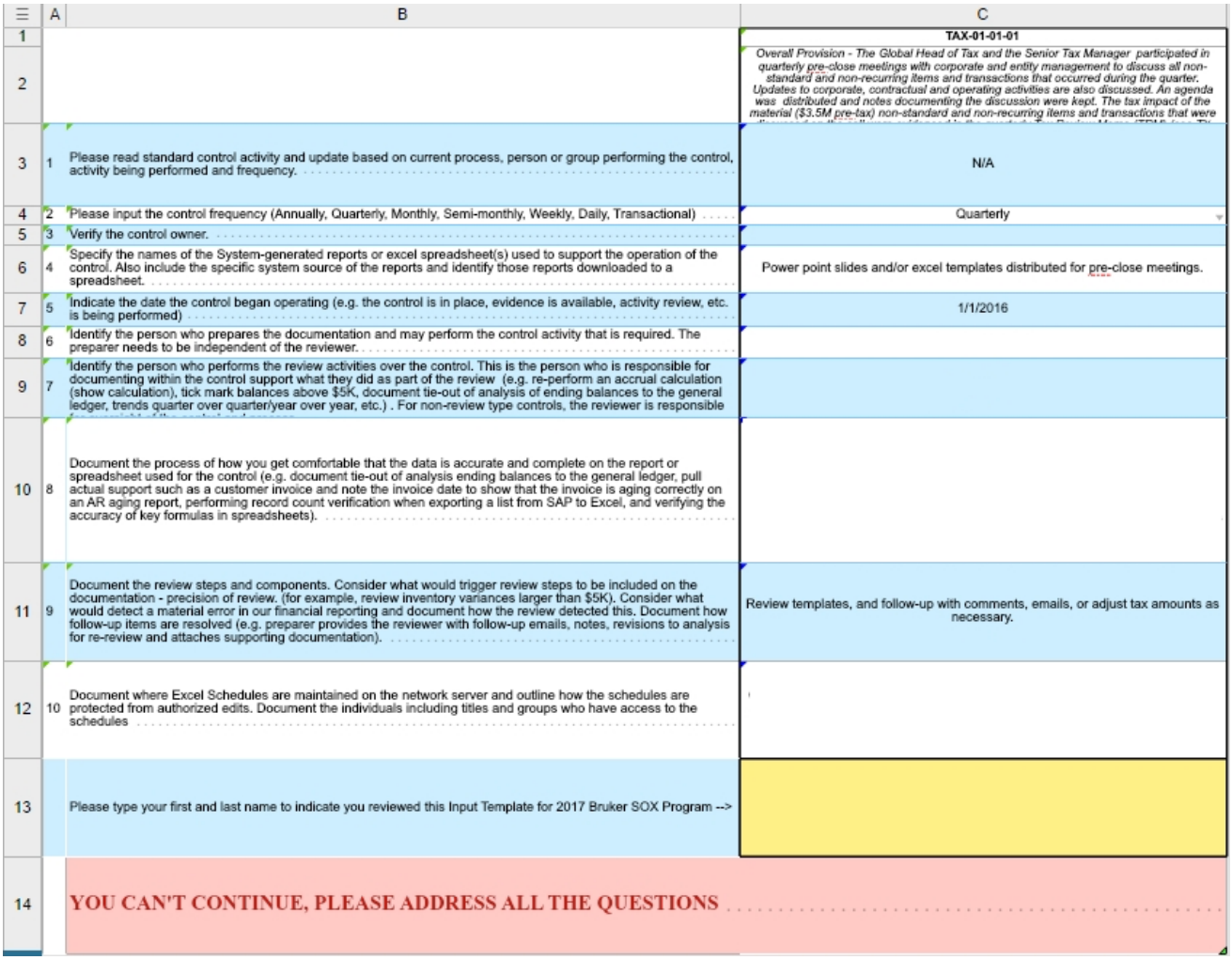
Issues that arose in past years of Bruker's Risk Management Program were:

(a) Control Owners were confused by the complete Risk and Controls Matrix structure;
(b) The follow-up with Control Owners for the successful update of the fields was manual and time consuming;
(c) The conflicts on versions due to not well regulated updates to the Excel RCM files were many and not easy to manage/resolve.

What the team thought in order to solve these problems was to move all the information in a web-based platform, enabling co-working on spreadsheets, ensuring the appropriate permissions setting and the easy collaboration through comments targeting the interested individuals. This platform is Workiva Wdesk.

In order to speed up the input and editing of the information, a Input Template was created. This, together with Wdesk linking capability, enabled the possibility of reaching each single Control Owner with targeted questions on a template with information cascading immediately into RCMs. The example of an Input Template can be seen in Fig.21. Part of my work was to create the Input Templates (1 for each control), manage the permissions of the platform and link the documents following the developed structure (Fig.16, p30).

Through the Input Templates the issue *(a)* was addressed by the team. Control Owners could now access a simplified interface (Fig.21) in order to update information on their controls. Information were forwarded to RCM via the linking feature of the platform.



	A	B	C
1			TAX-01-01-01
2			*Overall Provision - The Global Head of Tax and the Senior Tax Manager participated in quarterly pre-close meetings with corporate and entity management to discuss all non-standard and non-recurring items and transactions that occurred during the quarter. Updates to corporate, contractual and operating activities are also discussed. An agenda was distributed and notes documenting the discussion were kept. The tax impact of the material ($3.5M pre-tax) non-standard and non-recurring items and transactions that were*
3	1	Please read standard control activity and update based on current process, person or group performing the control, activity being performed and frequency.	N/A
4	2	Please input the control frequency (Annually, Quarterly, Monthly, Semi-monthly, Weekly, Daily, Transactional)	Quarterly
5	3	Verify the control owner.	
6	4	Specify the names of the System-generated reports or excel spreadsheet(s) used to support the operation of the control. Also include the specific system source of the reports and identify those reports downloaded to a spreadsheet.	Power point slides and/or excel templates distributed for pre-close meetings.
7	5	Indicate the date the control began operating (e.g. the control is in place, evidence is available, activity review, etc. is being performed)	1/1/2016
8	6	Identify the person who prepares the documentation and may perform the control activity that is required. The preparer needs to be independent of the reviewer.	
9	7	Identify the person who performs the review activities over the control. This is the person who is responsible for documenting within the control support what they did as part of the review (e.g. re-perform an accrual calculation (show calculation), tick mark balances above $5K, document tie-out of analysis of ending balances to the general ledger, trends quarter over quarter/year over year, etc.) . For non-review type controls, the reviewer is responsible	
10	8	Document the process of how you get comfortable that the data is accurate and complete on the report or spreadsheet used for the control (e.g. document tie-out of analysis ending balances to the general ledger, pull actual support such as a customer invoice and note the invoice date to show that the invoice is aging correctly on an AR aging report, performing record count verification when exporting a list from SAP to Excel, and verifying the accuracy of key formulas in spreadsheets).	
11	9	Document the review steps and components. Consider what would trigger review steps to be included on the documentation - precision of review. (for example, review inventory variances larger than $5K). Consider what would detect a material error in our financial reporting and document how the review detected this. Document how follow-up items are resolved (e.g. preparer provides the reviewer with follow-up emails, notes, revisions to analysis for re-review and attaches supporting documentation).	Review templates, and follow-up with comments, emails, or adjust tax amounts as necessary.
12	10	Document where Excel Schedules are maintained on the network server and outline how the schedules are protected from authorized edits. Document the individuals including titles and groups who have access to the schedules	
13		Please type your first and last name to indicate you reviewed this Input Template for 2017 Bruker SOX Program -->	
14		YOU CAN'T CONTINUE, PLEASE ADDRESS ALL THE QUESTIONS	

Fig.21 - Input Template - Example.

As it can be noted from Fig.21, a red cell asks the user to address all the questions in order to continue. The team didn't know how to control the completion of the Input Templates and I came up with the idea of using simple Excel functions in order to control the blank cells on the spreadsheet. This enabled a faster way to review the information updated by the control owner, by keeping under control the completion of the Input Templates.

This "control cell" was then linked to other spreadsheets and later became a KPI of the whole program. In-fact, the quantitative measure of "STATUS:COMPLETED" Input Templates and qualitative evaluation of the information provided were subject of reporting to management and financial leaders across the world (Fig.22).

	A	B	C	D	E	F
1					DATE	07/22/2016
2	Control Number	Control Owner	Status	Reviewed	Accepted	Info quality
3	GLFR-02-01-04		COMPLETED	YES	YES	GOOD
4	GLFR-05-01-01		COMPLETED	YES	YES	GOOD
5	GLFR-05-01-03		COMPLETED	YES	YES	GOOD
6	GLFR-05-01-05		COMPLETED	YES	YES	WORKABLE
7	GLFR-06-01-01		COMPLETED	YES	YES	GOOD
8	GLFR-07-01-01		COMPLETED	YES	YES	GOOD
9	GLFR-07-01-01a		COMPLETED	YES	YES	GOOD
10	GLFR-07-01-12		COMPLETED	YES	YES	GOOD
11	GLFR-07-01-25		COMPLETED	YES	YES	WORKABLE
12	GLFR-07-01-27		COMPLETED	YES	YES	GOOD
13	GLFR-07-01-28		COMPLETED	NO	NO	NOT SET
14	GLFR-07-01-29		COMPLETED	YES	YES	GOOD
15	GLFR-07-01-29a		COMPLETED	YES	YES	GOOD
16	GLFR-07-01-30		COMPLETED	YES	YES	WORKABLE

Fig.22 - Input Templates Review - Reporting.

Thanks to the Control cell and the possibility of adding comments (notified to the individual via email) to a targeted cell in the Input Template, the issue *(b)* was successfully addressed by the team. In addition, The requests to access the Input Templates and update the information were sent out using "Certification Letters", an add-on of Workiva Wdesk software. Certification letters offered a nice interface to automatically send kind reminders to Control Owners who did not certify the completion of Input Templates, enforcing automated follow up procedures thus maximizing the task completion.

The platform itself also provided a convenient feature to avoid misalignments on the information contained in the spreadsheets during updates, defined as issue *(c)*. This consisted in a "locking" of the Input Template whenever an authorized user was editing it. Users had to "SHARE" their changes when finished working and this would refresh all the links cascading the information through the documents structure.

4. Management Testing - Prepared by Client Lists

Prepared by Client Lists are used to collect evidences through the organization. Auditors from a hired third party company are preparing the list together with the Internal Controls team; the list is then rolled out to Control Owners of the legal entities in-scope of the Management Testing of Internal Controls, before the audit.

In Fig.23 it is possible to see the PBC List row structure, in Bruker SOX Program 2016.

Control #	Control Owner	Control Description	Additional Information	Period Requested	Date Due	Request	Attachment
GLFR-07-01-22	Claus	Regional Finance General Ledger Team, performs a monthly reconciliation of cash activities for the Cash Pooling Account, to ensure that all transactions were processed by the bank and that all transactions processed by the bank were properly recorded in SAP. Un-reconciled items are investigated and resolved timely. An independent member of the General Ledger team or Regional Finance Director will review the reconciliation monthly. Evidence of the review is indicated by sign-off on the Closing Checklist.	Locally maintained bank accounts with and are reconciled daily to the SAP accounts. The account is reconciled with the bank statement, the account with the data of the report EUROPEAN CASH-POOLING provided by corporate finance. The reconciliation is reviewed by the head of general ledger accounting and indicated by sign off from the head of general Ledger accounting or the legal entity owner.	March, May, and June	10/31/2016	1) Please provide monthly reconciliations	Please click on this cell, then open the right panel select the attachments section and attach a document, then select "File attached" from the options of this list.
					10/31/2016	2) Please provide approval of the reconciliations documented in the closing checklists	File Attached

Fig.23 - PBC List - row structure.

Issues that arose in previous years of Bruker's Risk Management Program were:

(a) Requests were not satisfied within the due date;
(b) Evidences of control and documents were not centrally stored;
(c) Requests were not matching the control performed (many differences across entities).

As for the Refresh Program (update of the RCMs) the request for the Evidences through PBC Lists was sent out using Workiva Wdesk "Certification Letters".
This led to having convenient follow up tools, such as the automated reminders feature that helped solving issue *(a).* Additionally, with respect to the requests satisfaction within the due date, a report of PBC Lists completion was developed. This was shown to Senior Management of the Company and was inserted in the KPI of the SOX Program.

The PBC spreadsheet on Wdesk also provided a central storage spot for all the collected evidences of each entity. Each Control Owner could actually attach the documents and evidences right on the spreadsheet in the "Attachment cell". This partially solved issue *(b)* as some evidences were too big to be scanned and uploaded. Auditors were thus able to request evidences, find them and audit them inside the same platform avoiding time and money wasting.

As a workaround to issue *(c),* the Internal Controls Team asked the hired third party audit company for the Management Testing to go through all the RCMs, reading the additional information on the controls, in order to ask for the appropriate audit evidence for the controls in the Prepared By Client lists.

5. Management Testing - Planning

The whole Bruker's Risk Management and SOX Compliance program was, for various reasons, missing a clear and detailed pathway to success in 2016. The Internal Controls Team was struggling to carry out the project without having a defined picture of what was already performed, what still had to be and the resources needed to complete the preparation work prior to testing.

This is why, when I joined the team, I drafted a Microsoft Project file that was able to organize the workflow on a daily basis tracking and monitoring the work of the team as a whole, and that of the external resources (third party audit firm, Control Owners in the various locations, PWC external auditors).

Task Name	Start	Finish	Deadline
BNN Requests draft Bruker China	Tue 6/28/16	Tue 6/28/16	NA
BNN Requests draft Bruker Singapore	Wed 6/29/16	Wed 6/29/16	NA
BNN Requests draft BBIO Switzerland	Mon 7/18/16	Tue 7/26/16	NA
BNN Requests draft BAXS US	Thu 6/30/16	Mon 7/4/16	NA
BNN Requests draft BDAL Gmbh	Mon 7/11/16	Fri 7/15/16	NA
BNN Requests draft BRKR HC	Mon 8/1/16	Mon 8/8/16	NA
BNN Requests draft US RF	Mon 7/11/16	Thu 7/14/16	NA
BNN Requests draft BAXS Gmbh	Mon 8/1/16	Thu 8/11/16	NA
BNN Requests draft Bruker UK	Thu 6/30/16	Fri 7/1/16	NA
BNN Requests draft Bruker Japan	Mon 7/18/16	Thu 7/21/16	NA
BNN Requests draft BOPT Gmbh	Fri 8/12/16	Wed 8/24/16	NA
BNN Requests draft BAXS France	Tue 7/5/16	Tue 7/5/16	NA
BNN Requests draft BNANO Gmbh	Tue 8/9/16	Mon 8/15/16	NA
BNN Requests draft BBIO US	Fri 7/22/16	Mon 7/25/16	NA
BNN Requests draft BNANO US	Wed 7/6/16	Fri 7/8/16	NA
BNN Requests draft BDAL US	Mon 7/4/16	Tue 7/5/16	NA
BNN Requests draft BEST EAS	Thu 8/18/16	Mon 8/22/16	NA
BNN Requests draft BBIO France	Tue 8/23/16	Tue 8/30/16	NA
BNN Requests draft Jordan Valley	Tue 8/16/16	Wed 8/17/16	NA
BNN Requests draft BBIO Gmbh	Thu 8/25/16	Tue 9/6/16	NA
BNN Requests draft BEST RI	Thu 9/1/16	Fri 9/2/16	NA
2nd Documentation review Bruker China	Thu 7/14/16	Fri 7/15/16	Mon 7/18/16
2nd Documentation review Bruker Singapore	Thu 8/4/16	Fri 8/5/16	Mon 8/15/16
2nd Documentation review BBIO Switzerland	Thu 8/11/16	Fri 8/12/16	Mon 8/15/16
2nd Documentation review BAXS US	Thu 7/21/16	Fri 7/22/16	Mon 8/22/16
2nd Documentation review BDAL Gmbh	Fri 8/12/16	Mon 8/15/16	Mon 8/22/16
2nd Documentation review BRKR HC	Thu 8/25/16	Fri 8/26/16	Sun 9/4/16
2nd Documentation review US RF	Wed 8/3/16	Wed 8/3/16	Sun 9/4/16

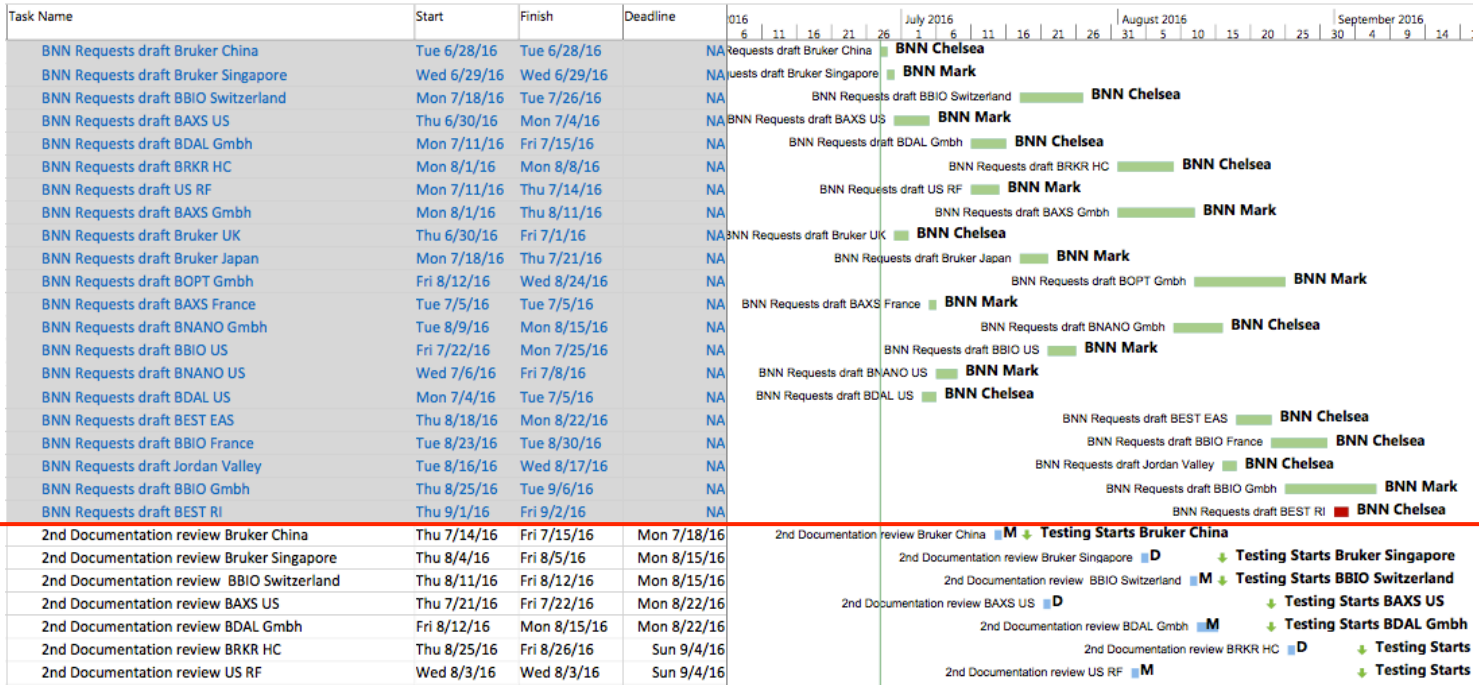


Fig.24 - Bruker's Risk Management Project - MSP

Due to the complexity of the document, Fig.24 only shows a portion of the whole Project. The project took into account 230 tasks, 4 major resources group, 21 in-scope testing locations.

The grey "BNN Requests draft" tasks in the left-upper part of Fig.24 are referred to the previously discussed review of each single location RCM, noting of the additional information for each control and drafting of the PBC List, performed by the third party audit firm. In order to organize the third party firm work in a suitable way, I negotiated a time budget per control with the "Principal in charge" of the company, then operated the product:

$$TE = NC \cdot TB$$

where:

NC = number of controls;
TB = time budget per control;
TE resulting in the amount of review time needed per entity.

A good solution regarding the order of the entities to take into account was found through a "Greedy algorithm" exploiting the heuristic problem solving theory. This isn't the optimal solution as heuristic methods do not guarantee the best solution but are a good and rapid approach to find a schedule that fits the purpose. The objective was to minimize the missing of deadlines (testing start) for all the entities, as shown on the bottom part of Fig.24.
The rule of the Greedy algorithm was:

"Highest ratio $\frac{TD}{TE}$ first",

where:

TD = task deadline converted in an ascending number;
TE = amount of review time needed per entity;

This moved the quickest reviews first but also considered the deadlines for longer reviews.
The scheduling worked nicely, making it possible to miss only one "testing start deadline".

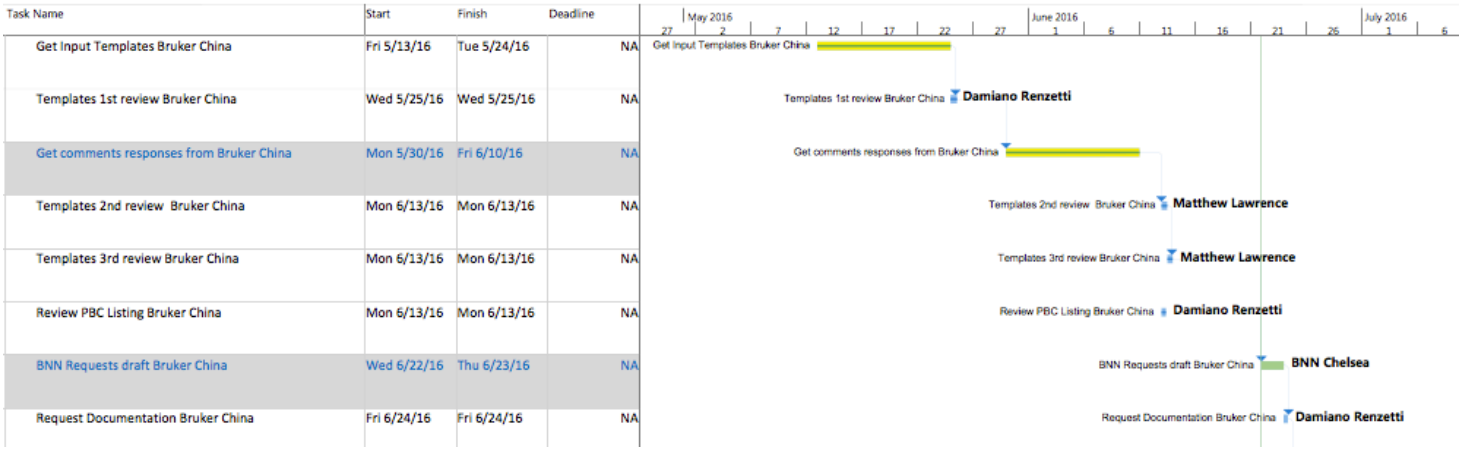


Fig.25 - Single entity (Bruker China) MS Project workflow

Progress was made measurable, transparent and well structured for each entity. This helped spreading the awareness on the program's milestones and objectives though reports that were sent out to General Managers of the in-scope locations, socializing dates and time endeavor. As shown in Fig.25, the workflow and progress of each entity could be easily filtered and communicated to interested individuals.

6. Management Testing - Audit

Risks and Controls Matrices and Prepared By Client lists were analyzed in previous sections. Those are referred respectively to the Refresh Program and the Management Testing preparation; it is now time to talk about the actual Audit process, and how the Management Testing is carried out on Wdesk. In order to do so we should introduce the Testing Sheets workbooks, stored in the platform one for each tested in-scope entity.

Fig.26 shows the example of a testing sheet, used to test controls within the in-scope entities each year. "Control" (green) and "Design" (dark blue) sections are linked to the RCM, thus every time authorized personnel edits the RCM the changes are set also on the single testing sheet.

Control	
Entity:	
Business Cycle:	INV
Process:	Inventory Movement & adjustment
Control Number:	INV-04-01-08
Standard Control Activity:	All inventory sub-ledger accounts are reconciled to the general ledger at least quarterly and are reviewed and approved by Finance Management.
Control Activity: Additional Information	Z530FI0001 report is extracted from BEP, with quantity and value by material. The balance by inventory account is compared with GL balance, to ensure inventory sub-ledger is reconciled to GL. The reconciliation is included in BS account reconciliation package.

Design	
Control Testing Technique:	Examination
Control Type:	Manual
Frequency:	Quarterly

Detailed Test Procedures/Attributes	
Attribute A:	Obtain the quarterly inventory reconciliation.
Attribute B:	Verify the reconciliation was approved by financial management.

Tickmark key:	
X	Attribute satisfied without exception.
F	Failed

Interim Testing	
Number of Exceptions:	0 exception(s)
Testing Status:	Complete
Operating Effectiveness:	Effective

	Description of Testing Selection	Date / Period	Attributes: A	Attributes: B	Sample Reference	Results 0 exception(s)	Remark
1	Z530FI0001 report; reconciliation; independent testing	31/03/2016	X	X	INV-04-01-08-201603-Inventory List and	Pass	
2	Z530FI0001 report; reconciliation; independent testing	30/06/2016	X	X	INV-04-01-08-201606-Inventory List	Pass	
3							
4							

Fig.26 - Testing Sheet example

"Detailed Test Procedures/Attributes" (light blue) on the other hand are locally stored on each testing sheet workbook for the sake of flexibility, and are reviewed/prepared by the third party audit firm that checks up-to-date additional information of the control on the same sheet. Fig.26 only shows a portion of the testing sheet, the Interim testing schedule; all the testing sheets are divided in "Interim Testing" and "Year-end Testing" schedules. This because if the Interim Testing fails for some reasons, it is a duty of the Internal Controls Team with the interested Control Owner to find a remediation to the ineffectiveness of the control and test it again during the year-end round. The remediation can consist of a performed Non-Key mitigating control that covers the risk of the failing Key control, or the application of auditors recommendations and a new test at Year-end (a control is anyhow considered remediated only if it is effective for a certain amount of time during the year).

"Interim Testing" (light blue) schedule shows the actual audit of the controls from the auditors, reporting description and references of samples selected, the satisfaction of the testing attributes for each sample and the remarks in case of exceptions. Four very important cells can be found in the testing sheets, and those are the "Number of exceptions", "Testing Status", "Operating Effectiveness" and "Recommendations". The latter is not shown on Fig.26. These cells are linked to the reporting, and through some filtering it was possible to provide a nice overview on the Results and Progress of the Management Testing.

Issues that arose in previous years of Bruker's Risk Management Program were:

(a) Progress was unclear, no information for corrective actions during the testing;
(b) Not all the information on the same spot for testing;
(c) Time consuming work in summarizing results.

One can easily see how issues *(a), (b), (c),* are solved through the use of the Wdesk Testing sheet shown in Fig.26. The "Testing Status" cell updating by the auditors made it possible to measure the progress of the testing, thus to monitor and manage Auditors and Control Owners during the process. All the information needed for testing, except audit evidences that could be found on the PBC List document, are coming with the testing sheet. Results are automatically rolled up and summarized thanks to the linking of Cells: "Number of exceptions", "Operating Effectiveness" and "Recommendation".

7. Results Collection and Reporting

Wdesk offers the possibility oh having real time up-to-date results and statistics across all the documents structure we already have seen. How?
Actually, the results and reporting come in the form of a presentation made of slides that is stored on Wdesk, and it is automatically updated by means of the links values that get changed inside the Testing Sheets, RCM and PBC Lists.

Testing results were summarized per business process (Fig.27), and also per legal entity(Fig.28).

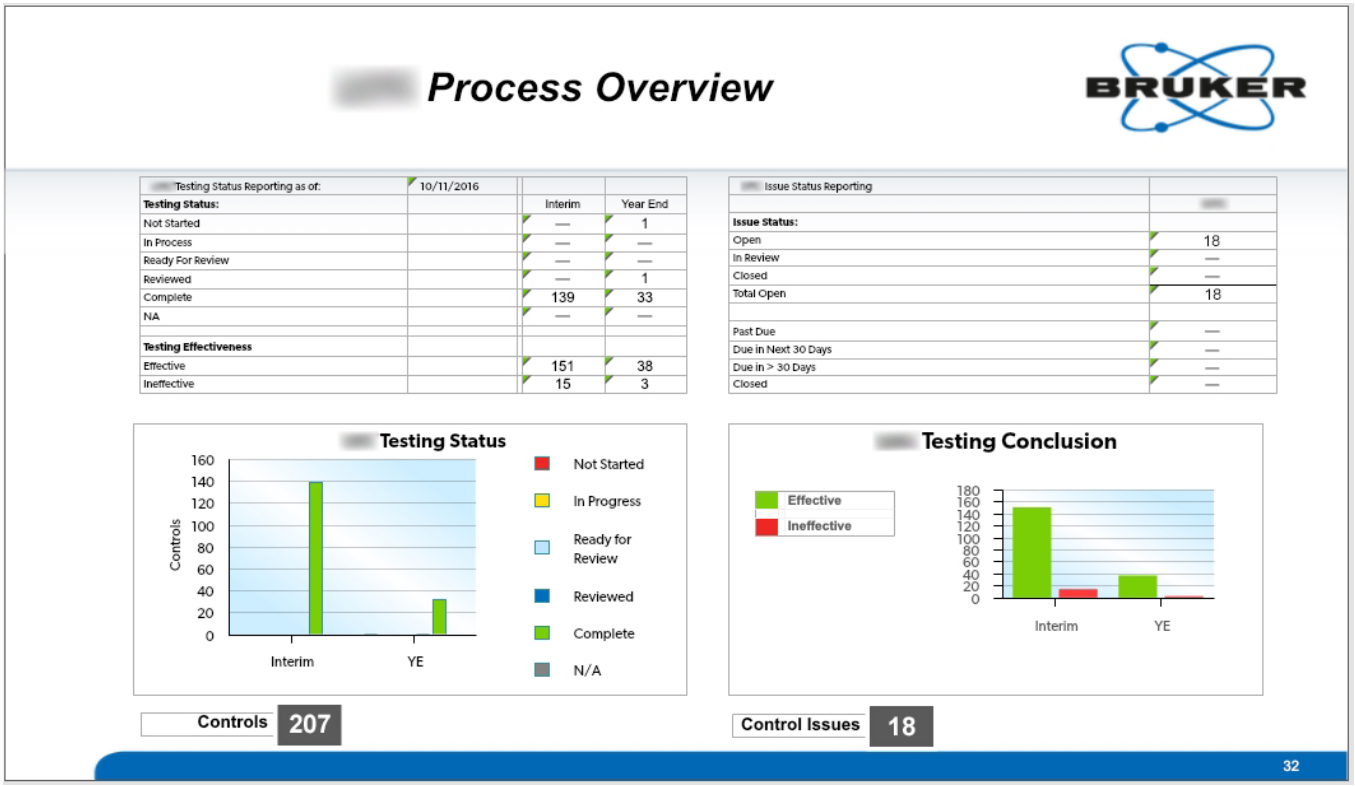


Fig.27 - Testing results per business process example

Obviously also global results were reported on the slides, ready to be printed whenever Senior Management or Governance of the company wanted an update. Focusing on single business processes though actually offers the possibility of understanding where to do better, where to enhance processes from a business and control point of view. In this example (Fig.27), the specific business process had approximately 9% of ineffective controls across the in-scope locations, a valuable information for corporate governance and an indicator for detailed investigations for the Internal Controls and Risk Management team.

Fig.28 - Testing results per business entity example

The testing results per business entity on the other hand, are a quality measure of the risk management program health status for each in-scope location. In this example (Fig.28), the entity did not really perform well, being that 16% of the controls are ineffective with respect of a considerably lower ineffective controls percentage in Bruker, globally.

Providing results this fast and in an automated way actually gives the possibility of building a "Heatmap" of the issues, and makes it possible to compare it with the following year management testing results. Issues and auditors recommendations automatically show up in "Local Summary Of Control Deficiencies" (LSOCD) lists, one for each entity. These are then consolidated into a global "Summary of Control Deficiencies" (SOCD) list; all of this happens automatically following the input of Auditors and their audit action.

This makes the framework the Team has created close to a Robotic Process Automation structure. There is a price to pay: the set-up of all the links across documents, and permissions and accounts management for the various parties joining efforts to carry out the annual routine. Despite this manual endeavor, the whole system raise efficiency also considering that once created it can be copied and rolled over for the forthcoming years risk management programs.

IV. Inside the Business

(1) Rationalization of a Legal Entity

1. Bruker Nano GMBH, Berlin, Germany

Bruker Nano Analytics (BNA) is a division of Bruker Corporation, and it is a leading manufacturer for analytical systems aimed to determine composition and structure of materials at the micro and nano scale. These can either be:

(a) Add-on for electron microscopy systems (SEM)

(b) Standalone, such as X-ray fluorescence spectrometers.[25]

Fig.29 - Bruker Nano Analytics Headquarters - Berlin, Germany

Bruker Nano Analytics designs and manufactures X-ray systems for elemental and structural analysis, including Energy and Wave-length Dispersive Spectrometers (EDS and WDS), Electron Backscatter Diffraction systems (EBSD), Micro-X-ray Fluorescence spectrometers (Micro-XRF) and total-reflection X-ray fluorescence analysis (TXRF) spectrometers.

The company was founded in 1991 as ROENTEC GmbH. In 2005 it was purchased by Bruker Inc. and is now part of its materials analysis business group. Bruker Nano Analytics employs almost 200 persons worldwide. Headquarters are in Berlin, Germany (Fig.29).[26]

Equipment of the Bruker Group is characterized by its reliability, user friendliness and application of innovative technologies. Bruker Nano maintains a quality management system which has been certified to fulfill the requirements of the DIN EN ISO 9001:2008 standard.[27]

2. Definition of “Rationalization”

What is the purpose of the Internal Controls and Risk Management structure?

As outlined in page13 of this document, Internal Controls can provide assurance that the objectives of an organization will be met, also controls and processes should be continuously monitored and evaluated for process improvement and fraud prevention. Ultimately, Internal Controls is about keeping control of the business leveraging every possible analysis from the collected data in order to avoid risks escalation into exploited vulnerabilities; and to make progress in processes and controls efficiency/effectiveness.

In order to do so the processes, controls, data collected should be consistent across the organization. In this way it is possible to compare results, measure performances, develop and apply best practices and improve the business quality.

What aforementioned in bold is the definition of “Rationalization” as it was intended in Bruker’s Internal Controls Team during my internship. Practically speaking a global set of Key Internal Controls was developed for Bruker Corporation, starting from a framework sponsored by PWC consulting company. Having this set of “standard controls”, the Internal Controls Team had to onboard entities across the globe by performing local Risk Assessments and walkthroughs, socializing the program with control owners and key individuals in financial/operations management.
This also means to build the discussed testing environment on Wdesk platform that is able to measure testing results, refresh information on the controls, store evidences centrally, provide time and money efficient ways to manage controls and audits.

It should be pointed out that Bruker Corporation, such as many other multinational companies, is constantly performing internal and external mergers and acquiring new emergent companies and businesses. This adds layers of complexity due to the need of globally shared processes and controls; and also, before year 2009, no global Internal Controls structure was present in Bruker Corporation as it was actually a large dimensioned family-run business.
In 2009 Bruker went public in the USA, being traded and creating the Bruker Holding Company that manages investor relations, shares and consolidated reporting. From that moment, the Internal Controls structure became necessary in every relevant location due to compliance to SOX Act. This started the process of spreading and sponsoring a “Corporate vision” of the controls, together with a Business Process (re)Organization initiative aimed to merge ERP systems, processes and practices among all the entities of the corporation.

Internal controls are anyway performed in “Non rationalized” Bruker legal entities, but they are not covering the same risks that Corporate considers Key and the controls descriptions are sometimes poor or not aligned with Bruker Holding requirements. These controls are called “legacy controls”.

During a rationalization, the legacy controls are analyzed and (where possible) mapped to standard controls. This often results in adopting the standard description of controls but reducing the number of those that are considered key, thus tested during the Management Testing.
The goal is to reduce costs, promoting a Lean and manageable structure but still keeping the business under control. If new controls are needed to cover Key Risk areas these are put in place with the due training and coaching of appropriate personnel, and then the Wdesk structure is built.

3. Build of Wdesk Structure for a legal entity

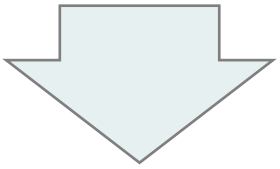
Let’s see how the Bruker Nano Analytics Legacy controls structure got rationalized and turned into a Standard controls structure during walkthroughs and meetings with the Financial Heads and control owners.

We can do so by comparing the Legacy controls list and the created RCM after the Rationalization process for one business cycle (in this example: FA - Fixed Assets). As it can be noted from a comparison of Fig.30 and Fig.31, the Legacy controls listed are 9, while the controls that are considered Key and thus are going to be tested during the first Management Testing after the Rationalization process are 5. In addition, one can see that the wording of the controls description changes as it is a lot less specific in the standard description of the controls. Standard language is in-fact not too specific in order to grant the possibility of using the same set in various legal entities; it can then be integrated with additional information when needed for the sake of understanding and auditor testing scripts definition (a general-worded control can result in a broad testing script including attributes that will most likely fail).

One other important difference sits on having the Standard controls mapped to Control Objectives (coming from the COSO Framework) and Associated Risks (Fig.31). This makes the audit from both Internal and External auditors easier, reduces time wasting in understanding if the business is under control and it is more professional than just having a simple list. When searching for mitigating and remediating controls for example it is possible to scroll the controls per Control Objective and/or per Associated Risk; it may exist a “Non Key” control that is performed but not tested (because non key) covering the same Associated Risk of an ineffective control.

Control Number	Current Control Activity Description
FA1	A fixed asset booked twice is automatically blocked by the system.
FA2	Each addition is checked by the head of accounting by comparing the SAP settings with the approved summary sheet.
FA3	Authorization policy for capital expenditures is implemented directly in SAP.
FA4	Head of Finance reviews assets under construction regarding capitalization obligation.
FA5	Depreciation is calculated automatically by SAP based on the underlying master data.
FA6	Double booking of monthly deprecation run is automatically blocked by SAP.
FA7	Head of Finance approves all disposals and scrappings with a net book value > TEUR 10
FA8	At the end of Q3 accounting department forwards a fixed asset register to the responsible employees and requests a confirmation of completeness.
FA9	Annual impairment test for assets with a net book value > TEUR 25 by the Head of Finance

Fig.30 - BNA Legacy controls list for Fixed Assets business cycle before the Rationalization.



Moving form a “Legacy controls” structure to a “Standard controls” structure

Control Number	Process	Control Objective ID	Control Objective	Associated Risk	Standard Control Activity	Risk Impact	…	…
FA-02-01-01	Master Data Maintenance	FA-02-01	All additions, changes and deletions to fixed asset master data are accurate, complete and authorized.	Asset Master Records may be set up or changed incorrectly resulting in incorrect accounting treatment and errors in financial reporting.	There are mandatory fields, default values, and non-changeable fields (i.e. asset class) for asset creation. Transactions which do not conform with these configurations generate an error message and cannot be completed until corrected.	Key Risk	…	…
FA-03-01-02	Acquisition	FA-03-01	Capital Project purchases are approved prior to a commitment being made by someone with the correct delegation of authority. Invoices for capital projects are approved by authorized individual prior to payment being made. All entries related to acquisitions are recorded completely and accurately.	Unauthorized / Invalid Capital Expenditure orders / invoices go undetected. Funds may not be available to finance the acquisition.	Capital Project purchases are reviewed and approved in accordance with the Corporate Fixed Assets Policy prior to being entered into the system.	Key Risk	…	…
FA-04-01-04	Depreciation	FA-04-01	All fixed asset depreciation amounts are posted completely and accurately to the ledger in a timely manner to ensure that information is recorded in the appropriate period.	Assets that are in-service may not be depreciated.	The accounting system is configured to begin posting depreciation in accordance with the Corporate Fixed Assets Accounting policy (in the month the asset is created).	Key Risk	…	…
FA-04-01-05	Depreciation	FA-04-01	All fixed asset depreciation amounts are posted completely and accurately to the ledger in a timely manner to ensure that information is recorded in the appropriate period.	Assets fully depreciated may incorrectly continue depreciation schedule. Assets may not be depreciated timely if not transferred from CIP timely. As a result, depreciation expense may not be appropriately reflected in the financial statements.	The system will not allow depreciation posting on fully depreciated assets and it has defined depreciation rules to prevent negative book values on assets.	Key Risk	…	…
FA-05-01-02	Retirement & Impairment	FA-05-01	Fixed asset disposals, retirements, and transfers are approved by appropriate personnel.	Lost, scrapped, transferred and/or sold assets may not be correctly identified and the detailed records may not be properly updated.	Asset disposals, retirements, write-downs (accelerated depreciation), and transfers are supported by authorized documentation and approved in accordance with delegation of authority levels outlined in Corporate Fixed Assets Policy.	Key Risk	…	…

Fig.31 - BNA Risks and Controls Matrix for Fixed Assets (FA) business cycle, after the Rationalization.

Once the legacy controls have been converted into standard, and a RCM with all the relevant information about the controls (including the Input Template questions shown in Fig.21 p39) is built, it is possible to start creating the documents structure in Wdesk for the newly rationalized legal entity.

The structure is explained in Fig.16 p30, and consists of the following documents related to the single entity, that need to be created from scratch (orange blocks in Fig.16):

- Risks and Controls Matrix
- Refresh Report
- PBC List
- Evidences Collection Report
- Testing Sheets
- Issues List
- Testing Results

The documents will have to be linked together and with other consolidated documents, this is done through copying and pasting cells from a “source” cell to a “destination” cell. A link can only have one source but multiple destinations. It is not possible to link formulas but it is indeed possible to link values of cells, that whenever updated modify numbers and information across the whole structure. The operation of copying and pasting links is simple but time consuming, and it takes a while to complete the build of the structure on Wdesk platform. After this operation is completed though, the rationalized legal entity will be part of the Risk Management program statistics and feed.

Obviously, as mentioned in page 30, also Permissions need to be assigned for each document and Users/Accounts Management needs to be performed for the users (control owners, internal auditors, external auditors) related to the new rationalized entity. New licenses need to be bought, users to be on-boarded and training to be performed.

(2) Turning a deficient Global Internal Control into an effective one

1. SAP Global Access Review

As described in page 10 (chapter *II - Corporate Risk Management),* part of the ITGC (IT General Controls) are related to the Access Control of the IT systems, so to ensure access to systems and data is restricted to authorized personnel.

In order to do so there are several IT products which are in many case not standalone systems but capabilities of a larger system and can be based on any or a combination of the following:

- User identity
- Role membership
- Group membership
- Other information known to the system

Access control includes any or all of the following: knowing who is attempting access, mediating access according to some processing rules, and managing where or how data is sent.[28]

Essentially, the Access control can be of two types:

- Identity-based Access Control. A security policy based on comparing the identity of the subject (user, group of users, role, process, or device) requesting access and the authorizations for this identity associated with the object (system resource) being accessed.
- Information Flow Control. Information flow policies dictate whether information with a particular characteristic can move from one controlled entity (container or subject) to another. Information flow control is based on some fundamental characteristic of the information (not the container), and might not involve an identifiable subject.[28]

When talking about SAP, the best Access Control default system without the implementation of further Business Solutions such as SAP GRC (Governance, Risk and Compliance) is:

RBACS, that stands for Role Based Access Control System

RBAC has emerged as a promising feature of many database management, security management and network operating system products. The essential advantage of RBAC products is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established

for each role; a user may belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without having to explicitly authorize each user to each resource.[28]

The SAP GRC business solution for a multinational company medium to large size (around 4000 SAP users) is very expensive, but as the US National institute of Standards and Technology (NIST) suggests, there are some organizational considerations to be made when choosing an Access Control system. Here are some of the questions an organization should ask itself when selecting an Access Control solution:

Organizational Considerations[28]

(i) Is the product necessary to adequately mitigate risk?

(ii) When selecting products organizations need to consider the threat environment and the security functions needed, to cost-effectively mitigate the risks to an acceptable level.

(iii) What is the impact on the training and level of effort needed to identify and define roles, the organizational impact of implementing roles, and the responsibility for role maintenance?

(iv) Has the impact on the enterprise operational environment where this product will operate been considered?

(v) Have security reviews included requirements for support, plug-in components, or middleware?

While my internship was ongoing, Bruker's chief officers were evaluating responses to these questions in order to understand if and when to put in place the SAP GRC solution.
The GRC solution would include a more sophisticated Access Control system (RBAC+ABAC, Attribute Based Access Control)[29], and also provide capabilities of review of the roles defined, of the conflicts due to segregation of duties controls, etc.

With no GRC implemented, an annual Global Access Review should be manually performed which means that each of the SAP users' roles should be reviewed from managers to ensure appropriateness. To perform such a review is a major endeavor for a 3500+ users, 450 managers audience. Aforementioned organizational considerations *(iii), (iv), (v)* should be took into account to better understand what a global review entails in an organization, in general.

Question *(iii)* considers the effort in training personnel on roles, in identifying and defining those on the system and the impact of implementation. Actually in Bruker the training offered to managers and users on roles and the access that was granted through them was not sufficient. Moreover, the identification and definition of roles is really a complex task and due to mergers, acquisitions and the contemporary use of 5 different versions of SAP; roles became buckets where access was thrown in when needed. Risky combinations of transactions were enabled, access was granted modifying a role for a small number of persons that needed it, but really it affected a larger audience, etc. This is however typical in large and complex organization, without sophisticated and expensive solutions such as the GRC.

What complexity does this add to the Access Review?

(1) Managers did not know roles, making it harder to accurately review them
(2) A “inappropriate” role could anyway include some access the user needed
(3) The change in a role could affect many users, also those not “tailored” for that role

Question *(iv)* considers the impact on the enterprise operational environment. In Bruker everything runs through SAP, unfortunately there are different versions of the system but everything is run through the system from Manufacturing to Customer support, Sales, Finance & Controlling, Inventory, Material Management, etc. With this scenario and the roles being defined in a bizarre way due to organizational history, resources and needs, moving a straw in the access domain could set up a timed bomb for the enterprise to be operationally shut down.

What complexity does this add to the Access Review?

(4) Removing roles from certain individuals could heavily affect enterprise operations
(5) Modifying roles could create a domino effect in the enterprise operations

Question *(v)* considers security reviews support, as far as software or plug-in components to perform a review both internal or external with respect to the system. Bruker did not have such tools and based its review on a list of users and their associated roles exported from SAP.

What complexity does this add to the Access Review?

(6) Low-value High-volume manual operations to perform the review
(7) Risk of stress burnout, due to limited human resources available
(8) Possibility of mistakes and misprints

Summarizing, trough analysis of the Organizational Considerations we can identify three main risks that are involved in performing the review:

1) Accuracy of the Access Review
2) Timeliness of the Access Review
3) Business Continuity after the Access Review

Unfortunately the External Auditor already stated the Access Control Review was a Significant Deficiency (see page 18) in 2015, due to the fact that almost every public company in the USA (according to the external auditor) are performing such a global review annually and Bruker was not. The Global Access review control was originally in place at Bruker, but due to lack of resources the control owner decided to stop performing the control in 2014 and the communication with the Internal Control Team somehow was not successfully handled.

The external auditor wanted to see a remediating action in 2016, so the team started working on a way to solve the situation in the quickest way possible. We only had 2 months to come up with a plan, send review sheets (270,000 Excel extracted rows for 3500+ SAP users, to be sent to 450 managers) record responses and elaborate changes on the system.

2. The current approach

The review was originally performed globally, with PDF review sheets created from SAP users/ roles table data extraction and sent through emails to the managers of SAP users.
Excel tracker files were used to keep record of the received responses from the managers and the process was performed with ***negative assurance***. This means that there was language on the review sheet stating that if the Manager did not respond to the email within 20days, all the roles were automatically considered as accepted and appropriate for the user.

Starting year 2014, the review stopped being global and was *only focused on Germany* (the country with most of the SAP users). A negative assurance protocol is not really accepted from the external auditor, moreover there was no risk-based reason to perform the review only in Germany. German users represented 25% of the whole users number, but still leaving 75% of the users not reviewed could not be considered acceptable risk-wise.

3. The proposed approach

After a week of team brainstorming and discussions on how to perform the Access Review, the topic was picked up from the BOD (Board Of Directors). This meant the priority of the issue was raised to the maximum level; we had to find a way to satisfy expectations. The team already came up with the idea of creating web polls to confirm the roles but the problem was sitting on the numbers.

We had 450 different polls with 270,000 different questions split among those. It was unfeasible and failing with respect to all the risk areas discussed before:

1) Accuracy of the Access Review,

   failing because 270,000 role/user combinations were too many to be reviewed;
   failing because of misprints and mistakes in creating polls;
   failing because data on manager-user association was not consistent/updated;

2) Timeliness of the Access Review,

   failing because creating 450 polls with 270,000 questions is time consuming;

3) Business Continuity during the Access Review

   failing because not having accuracy in the review could mean removing key roles.

The team was offered a terrific help from the IT department who suggested to remove “read only” roles with no authorization on editing data, bringing the questions down to 50,000 role/user combinations. Additionally, I personally found a method to compare SAP extracted data with the Active Directory of the company (mostly up to date) and with the global HR software (Fig.32).

Username	Name	Role	RoleDescr	Supervisor email	Supervisor Name
[redacted]	[redacted]	WW_XX_ITML_WEBUSER	Standart role for ITML-web-application	[redacted]	[redacted]
[redacted]	[redacted]	WW_BC_ENDUSER	Non-Critical Basis Authorizations for All Users	[redacted]	[redacted]
[redacted]	[redacted]	CH_B_SD_BILLING_PROCESSING	Fakturabearbeitung	[redacted]	[redacted]
[redacted]	[redacted]	CH_B_MM_ICB_ORDER	Maintain ICB Orders	[redacted]	[redacted]
[redacted]	[redacted]	WWVF_BKPF_BUP_FI	f_bkpf_bup star	[redacted]	[redacted]
[redacted]	[redacted]	CH_B_LO_ENGIN_CHG_MGMT	Maintain Engineering Change Management	[redacted]	[redacted]
[redacted]	[redacted]	WW_LO_ECH_MAINTAIN	Engineering Change Management	[redacted]	[redacted]
[redacted]	[redacted]	WW_BC_ENDUSER	Non-Critical Basis Authorizations for All Users	[redacted]	[redacted]
[redacted]	[redacted]	DECD_PLM	DECD_PLM	[redacted]	[redacted]
[redacted]	[redacted]	DECL_PLM	DECL_PLM	[redacted]	[redacted]
[redacted]	[redacted]	WWVD_EXPO_DEL_LOCK	Exportcontrol Delivery lock	[redacted]	[redacted]
[redacted]	[redacted]	WWV_EXPO_LOCK_ENDUSER	Exportkontrolle Enduser	[redacted]	[redacted]
[redacted]	[redacted]	WWVF_BKPF_BUP_FI	f_bkpf_bup star	[redacted]	[redacted]
[redacted]	[redacted]	WW_BC_ENDUSER	Non-Critical Basis Authorizations for All Users	[redacted]	[redacted]
[redacted]	[redacted]	WW_LO_ECH_MAINTAIN	Engineering Change Management	[redacted]	[redacted]
[redacted]	[redacted]	WW_BC_ENDUSER	Non-Critical Basis Authorizations for All Users	[redacted]	[redacted]
[redacted]	[redacted]	WW_LO_ECH_MAINTAIN	Engineering Change Management	[redacted]	[redacted]

Fig.32 - Clean data for Global SAP Access Review.

At this point we mitigated all the Accuracy related threats to the review, and also the Business Continuity issue dealing with the IT department on a quick rollback in case of a critical event.

It was my idea to use Wdesk and the Certification Letters software just as we did for the Refresh Program and the Management Audit (see pages 40-41). Actually there was no way to create a template with questions and copy it over for all the polls, having different questions for each poll. That's why I have developed a smart algorithm through macro recording techniques and coding, that works as a Software Robot, using iMacros browser automation software. The latter created polls automatically, starting from a list of questions in comma separated values format.

Having a robot to perform the creation of polls further reduced Accuracy Risk, and also mitigated Timeliness Risk. It still was a huge task to complete such a review in the 40 days left, due to the number of persons involved and the effort requested to complete the polls.

The software is analyzed in deep in next sections.

4. Robotic Process Automation

A software "robot" replicates the actions of a human being interacting with the interface of a computer or application. It can be the execution of data entry into an ERP system, or even a full end-to-end business process.[30] The software robot operates on the user interface (UI) miming a human interaction; this is a disruptive change from the traditional form of IT integration, which is based on Application Programming Interfaces (APIs).

SW robots are able to interpret the UI of applications and execute steps as a human user. They are programmed (or "trained") using demonstrative steps, like when creating a macro, rather than being programmed using code.[30] The intention is to provide an agile and configurable tool to non-technical users (business workers) in operational departments. A software robot should be seen as a "virtual worker" who can be rapidly trained by a business user in an intuitive manner, just as if he/she is showing steps to a co-worker or colleague. The benefit of this approach is quite impressive. It enables operations departments to self serve, implementing new technology without literally changing any technology they use. It also lowers the burden of IT professionals that can concentrate on more strategic IT implementations, such as ERP and BPMS (Business Process Management Systems) rollouts. RPA is classically seen as complementary to existing automation initiatives [31][32]

RPA's low requirement for technical support and high effectiveness explains why the idea of adoption typically starts from business operations teams and not from Information Technology (IT) departments.[32]

"RPA takes the robot out of the human. The average knowledge worker employed on a back-office process has a lot of repetitive, routine tasks that are dreary and uninteresting. RPA is a type of software that mimics the activity of a human being in carrying out a task within a process. It can do repetitive stuff more quickly, accurately, and tirelessly than humans […]"[33]

Leslie Willcocks, Professor of technology, work, and globalization at the London School of Economics' department of management.

5. Software Development

In order to automate the creation of web polls to be submitted to managers, HTML, Javascript, iMacros coding languages were used. Let's briefly analyze the developed software, starting from the HTML file launching the automation process(Fig.33)

```
<html>
<head>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
<script type="text/javascript" src="RPA_sw.js"></script>
</head>
<body>
<input type="file" name="filename" id="filename">
    <div id="csvimporthint"></div>
</body>
</html>
```

Fig.33 - HTML File launching the Javascript routine

The HTML page simply consists of a input type="file" making it possible to select a csv file that is pre-formatted and contains all the role/user/manager combinations sorted by manager. Simple but effective. The HTML language also loads the jQuery framework in order to be able to use a jQuery list of helping functions inside the script "RPA_sw.js".

```
$(document).ready(function () {
  $("#filename").change(function(e) {
    var ext = $("input#filename").val().split(".").pop().toLowerCase();

    if($.inArray(ext, ["csv"]) == -1) {
    alert('Upload CSV');
    return false;
    }

    if (e.target.files != undefined)
    {
```

Fig.34 - Javascript "RPA_sw.js" routine, CSV file opening 1

- In Fig.34, #filename is the file type input in the HTML document that calls this script, whenever it changes, the function at line 2 starts. If the selected file's extension is not ".csv" then the script displays a message that asks for a cvs file and exits.

```
12      var reader = new FileReader();
13      reader.onload = function(e)
14      {
15          var first=true;
16          var init=true;
17          var create=false;
18          var iiml = new ActiveXObject("imacros");
19          var iret
20          var test;
21          var rowNumber=e.target.result.split("\n");
22          iret = iiml.iimOpen();
```

Fig.35 - Javascript "RPA_sw.js" routine, CSV file opening 2

- In Fig.35, If the file exists and it is a CSV file, the FileReader instance gets created. When the file is loaded, some variables are defined and initiated. The rows of the CSV file get split (using new line "\n" as a separator) and loaded in the variable "rowNumber". NOTE: the instructions at line 18 and 22 create an instance of iMacros browser. That object will be used later to run the automation.

```
23          for (var j=1;j<rowNumber.length;j++)
24          {
25              var colNumber=rowNumber[j].split(",");
26              if (init)
27              {
28                  var currSupervisor = new String();
29                  var supervisorEmail = new String();
30                  var usernames = new Array();
31                  var nameOfUsers = new Array();
32                  var roles = new Array();
33                  var rolesDescr = new Array();
34                  currSupervisor=colNumber[5];
35                  supervisorEmail=colNumber[4];
36                  init=false;
37              };
38              if (currSupervisor==colNumber[5])
39              {
40                  usernames.push(colNumber[0]);
41                  nameOfUsers.push(colNumber[1]);
42                  roles.push(colNumber[2]);
43                  rolesDescr.push(colNumber[3]);
44              } else
45                  {
46                      create=true;
47                      init=true;
48                      j--;
49                  };
```

Fig.36 - Javascript "RPA_sw.js" routine, CSV file scan

- In Fig.36, The for cycle scans the entire CSV file, row by row (Note: this for cycle is the core of the algorithm and it includes all of the code). Each row is then split in columns using comma " , " as a separator and values are stored in “colNumber” array. If the supervisor stays the same (supervisor of the current row is stored in colNumber[5] variable as it is the 6th column in the csv file formatting), SAP users and their names as well as SAP roles and role description are saved in arrays which are: "usernames", “nameOfUsers”, "roles", “rolesDescr". Each time the supervisor changes "currSupervisor" (current supervisor) variable is updated; also, "create" and "init" variables are set to true. This causes the creation of the certification letter (web poll) and the initialization of the arrays. The variable "j" is decremented in order not to miss one row.

```
50      if (create)
51      {
52              var cont=25;
53              var app=new String();
54              app=currSupervisor.replace(/\s/g, "");
55              currSupervisor=currSupervisor.replace(/\s/g, "<SP>");
56              currSupervisor=currSupervisor.substring(0, currSupervisor.length-4);
57              test="CODE:\n";
58              test+="VERSION BUILD=11.5.498.2403\n";
59              test+="SET !PLAYBACKDELAY 0.6\n";
60              test+="SET !TIMEOUT_STEP 3600\n";
61              test+="TAB T=1\n";
62              test+="TAB CLOSEALLOTHERS\n";
63              test+="URL GOTO=https://app.wdesk.com/certifier/process/ahBzfndlYm/letters/\n";
64              if (first)
65                      {
66                              test+="PAUSE\n";
67                              first=false;
68                      };
69              test+="TAG POS=1 TYPE=SPAN ATTR=TXT:Add<SP>a<SP>Letter\n";
70              test+="TAG POS=1 TYPE=SPAN ATTR=TXT:Select\n";
71              test+="TAG POS=1 TYPE=INPUT:TEXT FORM=ID:use_template ATTR=ID:id_name ";
72              test+="4CONTENT=SAP<SP>Access<SP>Review<SP>-<SP>"+currSupervisor+"\n";
73              test+="TAG POS=1 TYPE=INPUT:SUBMIT FORM=ID:use_template ATTR=ID:go\n";
74              test+="TAG POS=1 TYPE=A ATTR=TXT:Create<SP>Certification\n";
75              test+="WAIT SECONDS=1\n";
76              test+="DS CMD=KEY CONTENT="+currSupervisor+"\n";
77              test+="TAG POS=1 TYPE=A ATTR=TXT:"+currSupervisor.toUpperCase()+app.toLowerCase()+"\n";
78              test+="TAG POS=1 TYPE=INPUT:SUBMIT ATTR=NAME:go\n";
79              test+="TAG POS=1 TYPE=A ATTR=TXT:Letters\n";
80              test+="TAG POS=1 TYPE=A ATTR=TXT:SAP<SP>Access<SP>Review<SP>-<SP>"+currSupervisor+"\n";
81              iret = iim1.iimPlay (test);
```

Fig.37 - Javascript “RPA_sw.js” routine, CSV file scan

- In Fig.37, at line 50 when the "create" variable is true, first the outline of the certification letter gets created. "cont" and "app" variables are used due to needs imposed by iMacros coding language. "currSupervisor" is modified for the same reason (<SP> needed instead of a blank character for spaces in iMacros language). "test" variable (line 57 to 80) contains iMacros code that was generated through macro recording techniques. iMacros "tags" specific HTML elements and interacts with them in web pages miming the human action (as reported in p58).

```
    iret = iim1.iimPlay (test);
        for (var t=0;t<usernames.length;t++)
        {
                usernames[t]=usernames[t].replace(/\s/g, "<SP>");
                nameOfUsers[t]=nameOfUsers[t].replace(/\s/g, "<SP>");
                roles[t]=roles[t].replace(/\s/g, "<SP>");
                rolesDescr[t]=rolesDescr[t].replace(/\s/g, "<SP>");
                test="CODE:\n";
                test+="VERSION BUILD=11.5.498.2403\n";
                test+="SET !TIMEOUT_STEP 3600\n";
                test+="SET !PLAYBACKDELAY 0.1\n";
                test+="SIZE X=1632 Y=852\n";
                test+="TAG POS=1 TYPE=SPAN ATTR=TXT:Add<SP>Question\n";
                test+="WAIT SECONDS=0.05\n";
                test+="DS CMD=KEY CONTENT=USER:<SP>"+usernames[t]+",<SP>"+nameOfUsers[t];
                test+="<SP><SP>-<SP><SP>ROLE:<SP>"+roles[t]+"<SP><SP>-<SP><SP>DESCRIPTION:<SP>"+rolesDescr[t]+"<SP>\n";
                test+="TAG POS=1 TYPE=SPAN ATTR=CLASS:ui-icon<SP>ui-icon-plusthick\n";
                test+="TAG POS="+(cont).toString()+" TYPE=INPUT:TEXT ATTR=* CONTENT=Keep\n";
                test+="TAG POS="+(cont+2).toString()+" TYPE=INPUT:TEXT ATTR=* CONTENT=Remove\n";
                test+="TAG POS="+(cont+4).toString()+" TYPE=INPUT:TEXT ATTR=* CONTENT=User<SP>not<SP>reporting<SP>to<SP>me\n";
                test+="TAG POS=1 TYPE=INPUT:SUBMIT ATTR=NAME:submit_button\n";
                iret = iim1.iimPlay (test);
                cont+=12;
        }
        test="CODE:\n";
        test+="VERSION BUILD=11.5.498.2403\n";
        test+="SET !TIMEOUT_STEP 3600\n";
        test+="SIZE X=1632 Y=852\n";
        test+="TAG POS=1 TYPE=INPUT:SUBMIT ATTR=NAME:go\n";
        iret = iim1.iimPlay (test);
        create=false;
                };
            };
    };
    reader.readAsText(e.target.files.item(0));
}

return false;

 });
});
```

Fig.38 - Javascript "RPA_sw.js" routine, Web poll questions creation

- In Fig.38 The inner for cycle creates all the content of the certification letter (web poll), inserting the questions for the current supervisor. Arrays that were created during the scan of the CSV file are used and joined with iMacros coding language. iMacros code creates the questions, note that "cont" variable is incremented to properly tag the correct input element in the HTML code, that varies by 12 each time a question is added (number found through HTML DOM exploiting techniques). The "create" variable is set to false again, and the algorithm re-starts from the CSV file scan. When the file ends, the algorithm stops executing actions and quits.

SAP Access Review - [redacted]

2016 SAP Global Access and Critical Roles Review

You are receiving this certification letter as the supervisor/manager of one or more SAP users. Please review their roles (access rights) selecting "Keep" or "Remove" for each role.

If you are not familiar with a specific role, you have the ability to check a Role with underlying capabilities within an Excel document stored on Sharepoint by clicking on the link described below. Some roles carry "change" or "transaction" capabilities which are considered "higher risk". Please consider if these type roles are necessary for the employee to continue performing their job activities before selecting "Keep" or "Remove".

Please electronically sign-off at the end of the review process.
Your progress is saved automatically every 30 seconds, you can access the review again from the email you received.

Link to the Excel file containing SAP roles detailed descriptions: ROLES DESCRIPTION

NOTE: If a user should be deactivated, please select "Remove" on all of its roles.
NOTE: If a user is not reporting to you, please select "User not reporting to me" on all of its roles.

USER: [redacted] - ROLE: UK_B_CS_CONDITIONS - DESCRIPTION: Maintain Conditions within Service

○ Keep ☑ Remove ○ User not reporting to me

USER: [redacted] - ROLE: UK_B_CS_LOGISTICS - DESCRIPTION: Logistics within Customer Service

○ Keep ☑ Remove ○ User not reporting to me

USER: [redacted] - ROLE: UK_B_CS_MANAGMENT_REPAIR - DESCRIPTION: Repair Orders Management

☑ Keep ○ Remove ○ User not reporting to me

USER: [redacted] - ROLE: UK_B_CS_MASTER_DATA - DESCRIPTION: Maintain Service Master Data

☑ Keep ○ Remove ○ User not reporting to me

USER: [redacted] - ROLE: UK_B_CS_MESSAGES - DESCRIPTION: Maintain Condition Records Messages

○ Keep ☑ Remove ○ User not reporting to me

*All times listed are in US/Eastern

Fig.39 - Web poll outcome Example

In Fig.39, a portion of a certification letter (web poll) is shown. The upper part, above the red line, consists of the Outline of the document. The lower part, below the red line, consists of the questions referred to the manager and his user/roles combinations.

Whenever signed, these certification letters were time-stamped and signed-off with account digital signatures from a platform with a license that was officially bought from Bruker's company. That's why auditors were really satisfied with the outcome and the approach used for the review in such a small timeframe.

6. Results

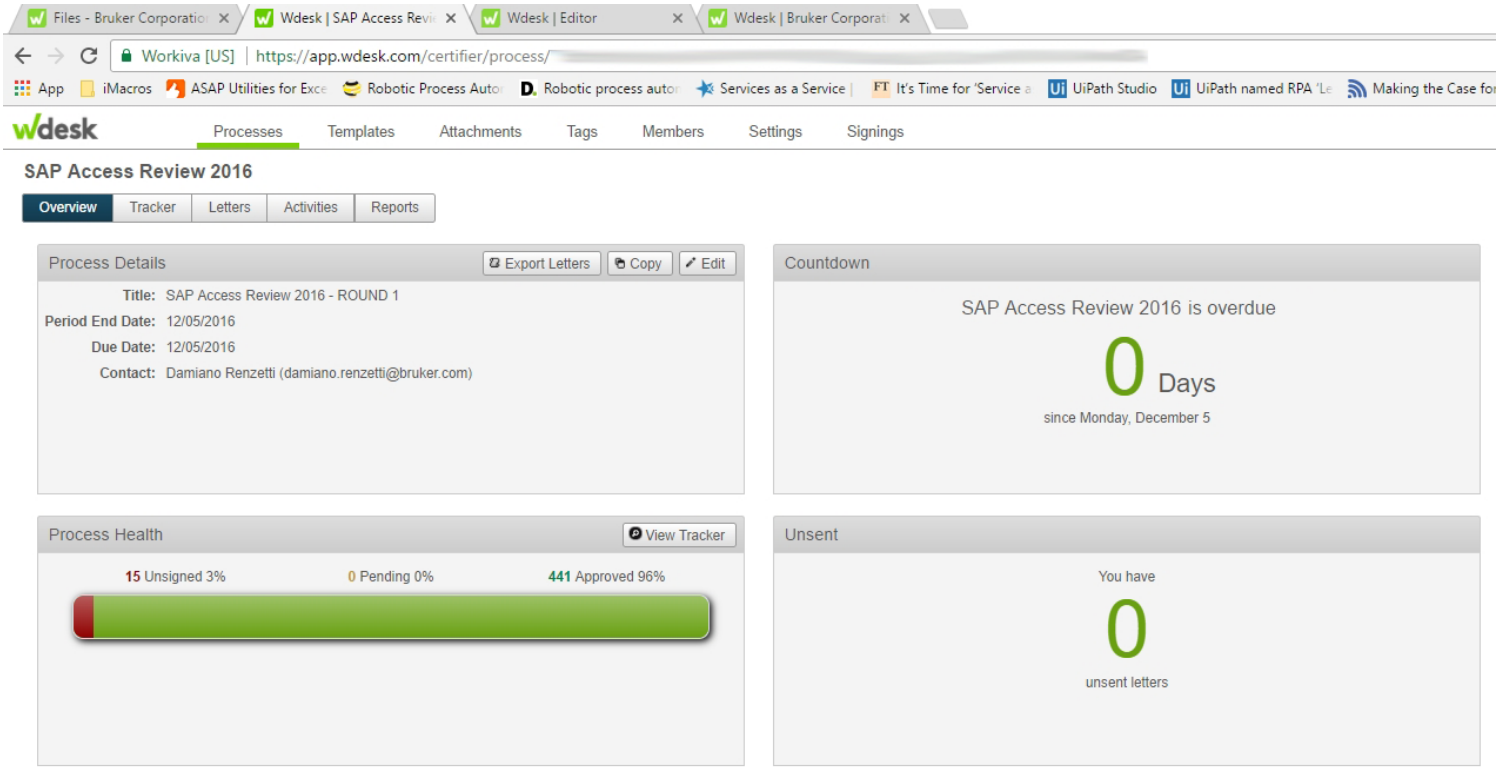


Fig.40 - Global SAP Access Control Review results.

In Fig.40 Results of the Access Review are shown. Using the developed approach the Internal Controls Team on behalf of the control owner of the Access Review Control was able to cover 97% of the company managers, implying 99% of the SAP role/user combinations reviewed.

This successful result was complimented by the BOD, and Senior Management of the company.

V. Conclusions

This experience has come to an end, and when sitting on a plane over the ocean one starts to think about what he learnt/understood/appreciated most.

This internship really opened up my mind, and almost surely set the direction of my next career moves. I deeply appreciated the very interesting mix between engineering knowledge and management skills required in such a position. I will certainly look for a job that brings these two sides together again, being very interested in the business and finance world and technically prepared in engineering.

I personally believe in the nearest future there will be a growing demand for engineers that are capable of developing business, of controlling it and making it more profitable. People that are able to negotiate, deal, express opinions, convince others, be leaders, be fair and believe in sustainability and in humanity. Activities such as team building, customers portfolio management, finance special operations, sales, cannot be run with mere knowledge. I think future engineers will not anymore mainly be focused in design and testing activities (where A.I. will progressively step in and win the competition) or any other kind of hard-skill activity like in the past. Speaking for myself I think engineers will soon be in the need of developing soft-skills in order to be successful in their careers. Stats show that robots are going to replace over 800 million jobs by 2030. Machines have more memory, more computational power, they are set to be potentially more “knowledge savvy” than humans.

As *Jack Ma*, founder of Alibaba recently said during the World Annual Economic Forum meeting in Switzerland (Davos, 2018-01-24):
”Computers are always going to be smarter than you are. When there’s a car, forget about running faster; when there’s a plane, don’t think you can fly like the plane. The same with computers, they never forget, they never get angry. […] People will need to develop soft-skills to compete with AI and be successful in the nearest future.”


POLITECNICO DI TORINO
1859
1906

VI. Thanks

I would personally like to thank every single person that made this life achievement possible.

This experience drove me through the completion of my studies teaching me that flexibility is one of the most important skills one could be spending to build a successful career. The following persons and titles aren't wrote down in any particular order, they all contributed to one of the most important experiences of my life:

Eric Saint Amour, Senior Manager Internal Controls @ Bruker,
The nicest person on earth, who cared for myself from the day we met;

Michael Knell, Chief Accounting Officer and VP of Finance @ Bruker
The manager everyone would like to have, never missed a shot;

Anne Rzegocki, Former Director Business Process Organization @ Bruker
My "American mama", always finds a way to make you smile;

Domizia Baldarelli, My fiancé
The one whose love made all of this possible, more than anything else;

Domitilla Renzetti, Full time sister
The sister everyone should have (if you have to have one);

Marco Renzetti, Best father in the world
The father that always supports and believes in you;

Fabiola Bolletta, Best mother in the world
The mother that cheers you up and makes you feel loved;

Jennifer Cui,
Matt Lawrence,
Liu Xiao, The interns crew!
I really miss you all guys, you made this journey full of happiness and warmth, and you paid all the lunches loosing at the credit card game.


POLITECNICO DI TORINO
1859
1906

VII. References

[1] - Wikipedia, The Free Encyclopedia, s.v. "Bruker," (accessed May 04, 2018) 'https://en.wikipedia.org/wiki/Bruker'

[2] - Bruker careers - Internal Controls Intern, Internship offer

[3] - Committee of sponsoring organizations of the three-way commission, (accessed May 04, 2018) 'https://www.coso.org/'

[4] - "Archived copy". Archived from the original on 2009-02-28. Retrieved 2009-04-21., "Internal Control— Integrated Framework"

[5] - 'PUBLIC LAW 107–204—JULY 30, 2002, 107th United States of America Congress'

[6] - U.S. Securities and Exchange Commission SEC, "What We Do", (accessed May 04, 2018) 'www.sec.gov'

[7] - "The Role of the SEC", (accessed May 04, 2018) 'www.investor.gov'

[8] - Public Company Accounting Oversight Board, (accessed May 04, 2018),'https://pcaobus.org//Inspections/Reports/Pages/default.aspx'

[9] - 'Rezaee, Zabihollah. Financial Statement Fraud: Prevention and Detection. New York: Wiley; 2002'

[10] - "Project Planning Tools - Popularity Ranking". Project Management Zone. Retrieved 6 August 2015

[11] - Van Decker, John E.; Iervolino, Christopher (May 2016). "Magic Quadrant for Financial Corporate Performance Management Solutions". Gartner. Gartner. Retrieved 28 September 2016

[12] - Kugel, Robert (July 2016). "Workiva Automates Composite Documents with Wdesk". Ventana Research. Retrieved 1 November 2016

[13] - Security and Exchange Commission (January 30, 2009). "Final Rule: Interactive Data to Improve Financial Reporting" (PDF). Release Nos. 33-9002; 34-59324; 39-2461. "Companies will provide their financial statements to the Commission and on their corporate Web sites in interactive data format using the eXtensible Business Reporting Language (XBRL)."

[14] - "Workiva product first to make Inline XBRL filing with SEC". Business Record. July 6, 2016. Retrieved October 30, 2016,

[15] - Compliance Week Blogs (April 3, 2015). "Workiva Adds New Feature to Wdesk for Sarbanes-Oxley Compliance". Compliance Week. Wilmington Compliance Week plc. Retrieved 30 October 2016

[16] - Konrad, Alex (October 13, 2016). "These Are The Top-Rated Public Cloud Companies To Work For According To Glassdoor". Forbes

[17] - "Fortune Top 10 Best Large Workplaces in Technology". Great Place to Work. September 14, 2016

[18] - Oleson, Joel (December 28, 2007). "7 Years of SharePoint - A History Lesson". Joel Oleson's Blog - SharePoint Land. Microsoft Corporation. MSDN Blogs. Retrieved August 13, 2011

[19] - SharePoint 2016, Team Collaboration Software Tools". products.office.com. Retrieved 2017-07-19

[20] - "SharePoint – Team Collaboration Software Tools". Microsoft Office. Retrieved 2015-05-19

[21] - "Company overview of Ipswitch, Inc.". Bloomberg. Retrieved June 29, 2016

[22] - "Ipswitch makes another tech acquisition:iOpus Software". Boston Business Journal. April 24, 2012. Retrieved June 29, 2016

[23] - "iMacros Feature Comparison - Free and Business Editions". iMacros website. Ipswitch, Inc. Retrieved 9 January 2011

[24] - "iMacros Macro or Script". iMacros wiki website. iOpus. Retrieved 17 March 2014

[25] - Microscopy and Analysis, s.v. “Bruker Nano Analytics” (accessed May 04, 2018) ‘https://microscopy-analysis.com/suppliers/bruker-nano-analytics'

[26] - Bruker Nano Analytics, Linkedin, (accessed May 04, 2018), 'https://www.linkedin.com/company/3312924/'

[27] - ChemEurope, s.v. “Bruker Nano GmbH”, (accessed May 04, 2018) 'http://www.chemeurope.com/en/companies/17548/bruker-nano-gmbh.html'

[28] - National Institute of Standards and Technology, Special Publication. NIST SP 800-36 Pages 16,17,18

[29] - SAP blogs, s.v. “A Hybrid Access control Model:RBAC+ABAC” by Anand Nayak Rao Kotti (accessed May 07, 2018) ‘https://blogs.sap.com/2015/07/07/a-hybird-access-control-modelrbacabac/'

[30] - Blue Prism’s robotic process automation offers scope for artificial intelligence, by Michael Azoff, Ovum, Retrieved Jun, 2015

[31] - Building a Center of Expertise to Support Robotic Automation, Forrester Consulting, Retrieved February, 2014

[32] - The Role of IT in Business Driven Process Automation, Forrester Consulting, Retrieved July, 2011

[33] - The next acronym you need to know about: RPA (Robotic Process Automation), by Xavier Lhuer, Mckinsey, Retrieved December, 2016

Additional References

- Wikipedia, The Free Encyclopedia, s.v. “Internal Control" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/Internal_control'

- Wikipedia, The Free Encyclopedia, s.v. “U.S. Securities and Exchange Commission” (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/U.S._Securities_and_Exchange_Commission'

- Wikipedia, The Free Encyclopedia, s.v. “Public Company Accounting Oversight Board" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/Public_Company_Accounting_Oversight_Board'

- Wikipedia, The Free Encyclopedia, s.v. “Microsoft Project" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/Microsoft_Project'

- Wikipedia, The Free Encyclopedia, s.v. “Workiva" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/Workiva'

- Wikipedia, The Free Encyclopedia, s.v. "SharePoint" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/SharePoint'

- Wikipedia, The Free Encyclopedia, s.v. "iMacros" (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/IMacros'

- Wikipedia, The Free Encyclopedia, s.v. “Ipswitch, Inc.” (accessed July 10, 2018) ‘https://en.wikipedia.org/wiki/Ipswitch,_Inc.'