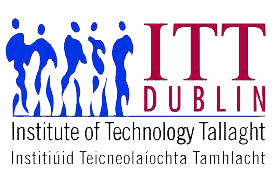
ISO 27001 Mini Project



Student No: X00112018

Student Name: Dylan Byrne

Contents

[1 Introduction 3](#_Toc468224657)

[2 What is ISO 27001 3](#_Toc468224658)

[3 Asset Register 4](#_Toc468224659)

[3.1 What Is an Asset Register 4](#_Toc468224660)

[3.2 Importance of an Asset Register 4](#_Toc468224661)

[3.3 Building an Asset Register 5](#_Toc468224662)

[3.4 Asset Owner 6](#_Toc468224663)

[3.5 Work Performed 7](#_Toc468224664)

[4 Risk Assessment 8](#_Toc468224665)

[4.1 Twelve Key Elements of a Risk Register Template 8](#_Toc468224666)

[4.2 Development of a risk register 11](#_Toc468224667)

[4.3 Risk Mitigation 12](#_Toc468224668)

[5 Policies and Procedures 13](#_Toc468224669)

[5.1 Importance of Policies and Procedures 13](#_Toc468224670)

[5.2 Implementation of Policies and Procedures 13](#_Toc468224671)

[5.2.1 Requirements 13](#_Toc468224672)

[5.2.2 Risk Assessment 14](#_Toc468224673)

[5.2.3 Optimization 14](#_Toc468224674)

[5.2.4 Structure of Documentation 14](#_Toc468224675)

[5.2.5 Approval 15](#_Toc468224676)

[5.2.6 Employee Awareness 15](#_Toc468224677)

[5.2.7 Maintenance 15](#_Toc468224678)

[6 ISO 27001 Audits 16](#_Toc468224679)

[6.1 Gap Audit 16](#_Toc468224680)

[6.2 Stages 16](#_Toc468224681)

[6.2.1 Stage One 16](#_Toc468224682)

[6.2.2 Stage Two 16](#_Toc468224683)

[7 Business Operations 17](#_Toc468224684)

[7.1 Infrastructure 17](#_Toc468224685)

[7.2 Organisation 17](#_Toc468224686)

[7.3 Business 17](#_Toc468224687)

[8 References 18](#_Toc468224688)

# Introduction

This document has been created with the intent to outline what ISO 27001 is as well at the importance of compliance to such a standard within the working world. This document will explain some of the processes a company must go through to obtain an ISO 27001 certificate and more importantly processes in which I have had a hand in. Hopefully this document will enlighten the readers of why such a certificate is beneficial to business.

# What is ISO 27001

According to IMSM ‘ISO 27001 sets out the requirements of information security management systems’ in relation to ‘information and cyber security’ offering a comprehensive set of controls based on the best practice in relation to information security (IMSM, 2015). ISO 27001 is a set security standard set by the International Standard Organisation (ISO) (Advisera, 2016).

ISO 27001 has been updated since its release back in 2005 and the latest revision of the new ISO 27001 standard was published back in 2013, where it was given the new title ISO/IEC 27001:2013 (Advisera, 2016). ISO 27001 was developed with the basis of the British standard BS 779-2. (Advisera, 2016). ISO was written by the world’s best experts in the field of information security, and has the ability to be introduced into any kind of working environment and organization whether they be profit or non-profit, private or state-owned, small or large (Advisera, 2016).

ISO offers a guideline for businesses to follow with the interest of providing the best possible practices that have been proven to help minimalize risk to a business and help protect their data and information. By becoming ISO 27001 compliant the company therefore employs a certain high level of security and are in return given a certification ‘which means that an independent certification body has confirmed that an organization has implemented information security compliant with ISO 27001’ (Advisera, 2016). This in turn can end up giving potential clients an ease of mind and the confidence that the stored data they may need to give will be looked after and protected.

It should be noted that ISO is not a once off activity but a regular and routinely exercise that must be constantly looked at and supervised usually done via ‘Regular audits ensure your organisation continues to meet its obligations regarding data security and keeps your staff focused on the importance of complying with standards’ (IMSM, 2015).

# Asset Register

While working on ISO 27001 I was given a multitude of tasks that needed completion among those items was an Asset Register this in turn turned out to be the largest project I would work on for the ISO 27001.

## What Is an Asset Register

An asset register is a means for a company to control and monitor the assets of the business. To define what an asset is correctly according to the 2005 revision of ISO/IEC 27001 an asset is defined as anything of value to the organization (Kosutic, 2016).

As such an asset covers a rather broad view and therefore quite a number of items can be entered within the register. According to Dejan Kosutic ‘since ISO 27001 focuses on preservation of confidentiality, integrity and availability of information’ (Kosutic, 2016). As such assets to an organisation include

* The Hardware – Hardware include but are not limited to Laptops, Desktops, printers, scanners, mobile phones, etc.
* Software – Development software, paid for software, free software, etc.
* Information – Information stored such as databases, documents, excel and physical information such as invoices letters, etc.
* The Infrastructure – Utilities, the office to name a few.
* ‘People are also considered assets because they also have lots of information in their heads, which is very often not available in other forms’ (Kosutic, 2016).
* Outsourced Services – Such as the cleaner, suppliers, etc.

## Importance of an Asset Register

It is important for a company to have an asset register so as to monitor all assets owned by the business. Keeping track of a company’s assets is a must reasons being that by recognising current asset holders responsibility of the assets can be delegated correctly and the ‘protection of confidentiality, integrity and availability of the information’ (Kosutic, 2016) can then be delegated to those same people who can then be held accountable for any risk to the business, which in turn helps mitigate risk as employees will be more careful with handling sensitive information as they are now responsible for all assets they are in charge of.

While speaking about risk another reason why asset registers are so important to a business is brought to attention by Mr Kosutic who explains that assets are usually key in performing a risk assessment, as they help to identify risks to the business along with threats and vulnerabilities. (Kosutic, 2016).

## Building an Asset Register

If an asset register was not previously developed, Mr. Kosutic explains that the easiest time to do so is during the initial risk assessment process, provided the chosen methodology is an asset-based risk assessment, as this is the preferred moment where all assets to a business need to be identified along with the owners of said assets (Kosutic, 2016).

Although according to Vigilant software who in their words state ‘asset-based risk assessment are still widely regarded as best practice, and present a robust methodology for conducting risk assessments’ it is no longer an essential requirement under ISO 27001:2013 and it is now up to the discretion of the business to choose a relevant risk assessment methodology (Vigilant, 2016).

The best way to begin building an asset register in Mr Kosutic eyes is to interview the head of all the departments within the organisation and list the assets used by each department. This is a method that was conducted within All n One when performing the task of updating the asset register. However instead of asking heads of the department due to All n One as a company being on the smaller and more easily intractable side of a business all members of the business were interviewed for the assets they use, when given the chance.

Mr Kosutic explains an easy technique that can be used is the ‘describe-what-you-see technique’, a technique simplistic in both view and execution yet rather effective especially when considering the building of the asset register. He explains the technique works by ‘basically, ask this person e.g. to list all the software that he or she sees that are installed on the computer, all the documents in their folders and file cabinets, all the people working in the department, all the equipment seen in their offices, etc.’ (Kosutic, 2016).

ISO 27001 does not set out which details are needed for the asset register, Mr Kosutic stating that a person may only list the asset name and its owner but goes on to explain that one can also ‘add some other useful information’ such as the assets category, the location of the asset, some notes simply regarding the asset, etc.

Although Mr Kosutic states that the building of the asset register is usually left to the person who is in charge of coordinating the ISO 27001 implementation project which is usually the head of security (Kosutic, 2016), this is however not always the case as the work may be delegated and someone else may be asked to update or create the asset register, for example I was giving the task to update the asset register and I may have been given such a chance due to an asset register already having being built and that I worked under the supervision of the head of security.

## Asset Owner

The Asset owner is defined as an individual or an entity that is responsible for the ‘control, controlling the production, development, maintenance, use and security of an information asset’ (Vigilante, 2016).

Outlining what asset belongs to who is important information that must be included in an asset register the reason being the liability of the assets and control of said assets will fall onto the user.

The Owner of an asset is usually chosen as the one who operates and interacts with the asset, they are also made to make sure that the information related to an asset is protected (Kosutic, 2016).

An example of an asset owner given by Mr Kosutic is as follows ‘an owner of a server can be the system administrator, and the owner of a file can be the person who has created this file; for the employees, the owner is usually the person who is their direct supervisor’ (Kosutic, 2016).

For Certain assets that are used by more than one person on a regular basis such as printers or scanners, software, the asset owner can be delegated to whoever may be the head of the department that makes use of the asset or ‘can be a member of the board who has the responsibility throughout the whole organization’ (Kosutic, 2016).

## Work Performed

As mentioned previously while working with ISO 27001 I was given the task of updating the currently asset register. As such to begin with my work I had a look at the current asset register they had and what needed to be done to bring it up to date. The asset register was laid out in an excel spreadsheet with different tabbed pages for each individual section such as the hardware, software, etc.

The starting point for the asset register was decided to be updating the hardware section as this did not need as much work done to it as it was relatively up to date with the exception of several new computers that had recently arrived. To begin an email was sent around the company letting the owners of the new machines to notify me when they were going on break this was done as so to minimalize the impact I would have on their work. While on break with their permission I would take a screenshot of their current system specifications as well as a list of installed programs and lastly I would also retrieve the machines system tag to identify the computer via the BIOs. All this information was taken and then entered into the Asset register under the correct headings.

The reason for taking this information was rather simple it was done so as to uniquely identify this machine using the service tag of the machine which was then linked to the user who is in charge of said machine taking full liability. The reason for taking down the specs and software installations was to allow the ease of seeing what we currently have as a company.

The next section involving software required the version of software and product key if applicable. Using previous information I gathered in the form of software installations I was able to retrieve the installed software and version and enter tem into the Asset Register.

Retrieving product keys were of a more difficult task however. Due to security viewing security keys is not as easy as opening up a piece of software and looking at the properties section, to get the keys I used an application called Produkey. Produkey would retrieve the product keys of all installed software; from there it was simply a matter of adding them to the register as well as any information in reference to them.

# Risk Assessment

Once all the assets have been properly documented and the information has been stored within the Asset Register, the next thing to do is to identify the potential threats and ‘vulnerabilities that could pose’ a risk to those assets (Vigilant, 2016).

Once the threats have been identified, it is time to perform an analysis of the risks, to ‘establish the impact level of the risks’ as well as the likelihood of it occurring (Vigilant, 2016). ‘The impact value needs to take into consideration how the Confidentiality, Integrity and Availability of data can be affected by each of the risks’ (Vigilant, 2016).

There are other fields that must be taken into consideration too such as the ‘legal, contractual and regulatory implications of risks, including the cost of the replacement of the asset, the potential loss of income, fines and reputational damage’ (Vigilant, 2016) as these will all have an impact on the business as a whole.

To Keep track of risks to the business they are recorded in an item known as the risk register or risk log. The risk register or risk log can be considered to be similar to the asset register with the difference being that a risk register stores all information on potential risks or threats to the business rather than items of value to the business.

## Twelve Key Elements of a Risk Register Template

When developing the risk register there are twelve key elements used that should be kept in mind when carrying out the risk management process and help with a risk assessment. According to Kloosterman these twelve key elements are as follows

1. Risk Category – This element refers to the categorisation of the scope such as where does it fall under. Does it fall under the category of scope, time, cost, resources, environmental, or another key category? Using these categories helps tease out likely risks and groups them into relevant categories for future reference.
2. Risk Description – Refers to simply a brief description of the potential risk.
3. Risk ID – Refers to a unique Identifier given to the risk to help identify and track it within the risk register. ‘If Resources is Category 8, then the first risk identified in this category has a unique ID of 8.1.’ (Kloosterman, 2013).

‘Elements 4 to 6 record the results of the Risk Analysis phase’ (Kloosterman, 2013).

1. Project Impact – A brief account detailing the impact the potential risk may have on a project associated with it. Impact may include, increase in cost/budget, more time needed, scope of project may fail to be achieved.
2. Likelihood – Refers to how the estimated chance of the potential risk occurring at some point and become an issue. This can be equated to the labels high, medium or low, but can also be placed on a number based scale if enough information is known. An example includes ‘resources have been over-committed in the past and we assess the likelihood of occurrence as High.’ (Kloosterman, 2013).
3. Consequence – Should the potential risk become an issue this refers to the impact or consequence of the potential risk on the respective project.

‘Elements 7 and 8 record the outcomes of the Risk Evaluation phase’ (Kloosterman, 2013).

1. Risk Rank – Refers to the ‘magnitude of the level of the risk’ (Kloosterman, 2013), it combines the elements five and six (likelihood and consequence) and gives it a rank respective to the other two ranks such that if both likelihood and consequence were both high than the risk rank too would also be labelled high.
2. ‘Risk Trigger – What are the triggers that would indicate the need to implement contingency plans? “If resource conflicts have not been resolved three weeks before the scheduled start date, then implement contingency plans.”’ (Kloosterman, 2013).

‘These last four elements record the outcomes of the Risk Treatment phase’ (Kloosterman, 2013).

1. Prevention Plan – A planned procedure that is created with the view of preventing the risk from occurring in mind. For example if resources in the past have been over committed than planning thoroughly and discussing what resources are needed before assigning resources may help prevent the risk from occurring.
2. Contingency Plan – Should the risk occur this plan is created to address the issue and minimalize its impact.
3. Risk owner – Refers to the person responsible for not only managing the risk but also implementing the course of action to both prevent and address with the potential risk.
4. Residual Risk – After the risk has been resolved by implementing either plan this refers to the risk that remains after.

## Development of a risk register

As mentioned before when creating the risk register one must discern the level of risk vs the likelihood this will help discern the potential threat it has on a business. Due to security risks I am unable to show the risk register of All n One however I am able to present the risk rating matrix that was used to help develop the risk register.

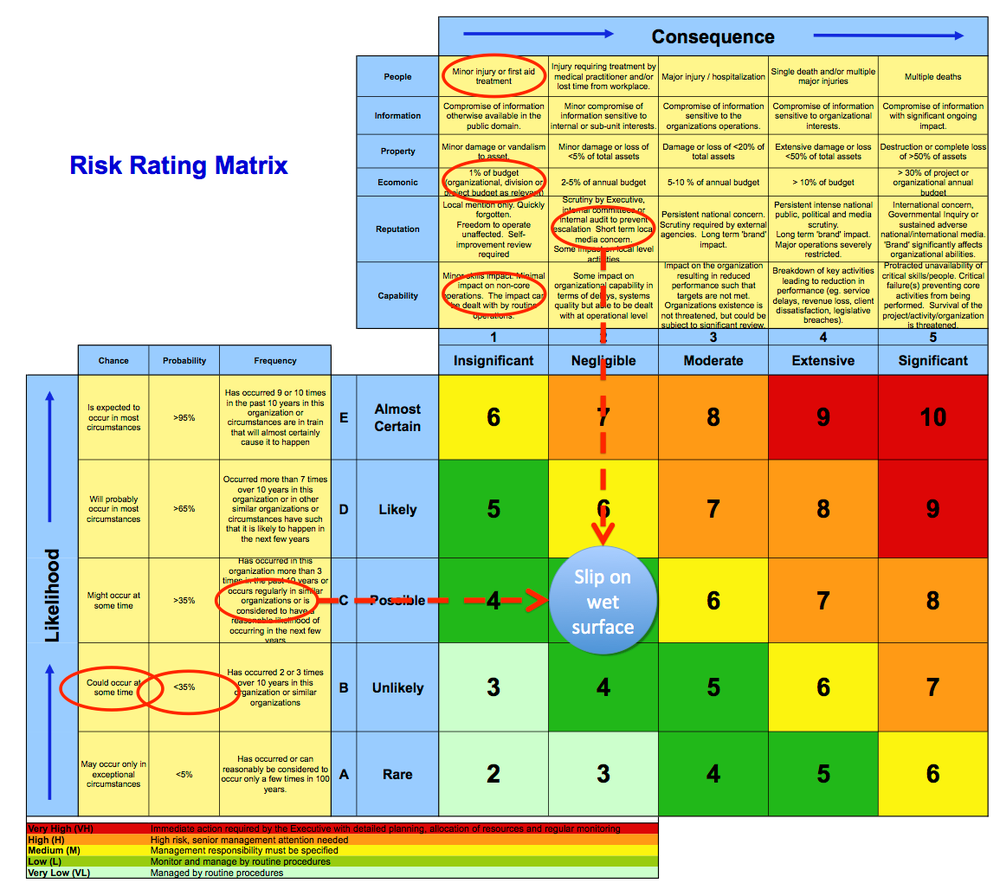


Fig 1.1 (Jakeman, 2016)

As can be seen from the image above the severity of the risk is generated via the consequence in correspondence to the likely hood of it happening. Using this method All n One is able to generate a risk register by comparing the consequence of the risk versus the likelihood.

## Risk Mitigation

Probably the most important part and the result of the risk assessment is to develop countermeasures to help reduce the likelihood of the risk happening. This is called risk mitigation. Risk mitigation is defined as the ‘process of developing options and actions to enhance opportunities and reduce threats to project objectives’ (Risk mitigation planning, implementation, and progress monitoring, 2013). This doesn’t mean the risk is removed entirely just reduce the chance of it occurring and the impact it may have on the business.

An example of a risk to a company such as shown in the risk rating matrix was a wet floor. A potential mitigation to that would involve putting up signs to announce the floors are wet so people would be more cautious, it does not remove the possibility of it happening however it does help reduce the possibility of it occurring if people chose to not ignore the sign.

For the risk register each risk would have a potential mitigation against it to help reduce the impact of it. This allows companies such as All n One to deal with such risks in a respective manner.

# Policies and Procedures

Before being able to obtain ISO 27001 companies must develop standard policies and procedures to deal with certain scenarios. These policies and procedures must be maintained and adhered to by all staff of the company.

For example while working at All n One several standard procedures were created in accordance to handling the asset register such that, should new assets arrive they are to be handled in a certain way that causes the items to be added to the asset register before being added to the secure location for storage.

## Importance of Policies and Procedures

Policies and procedures are a very important aspect of any business, ‘well-written business policies and procedures allow employees to clearly understand their roles and responsibilities within predefined limits’ (Company policies and procedures, 2011). What this means is that employees are able to follow these predefined policies and procedures to complete the work they are assigned without the constant guidance of management.

As such within a small company such as All n One where there is a constant workflow the development of these policies and procedures allow the members of staff to work without interruption and allow the senior managers to move on with their own work.

## Implementation of Policies and Procedures

When developing policies and procedures for the company there are some key steps that will help the process go smoother.

### Requirements

This should come as no surprise but when developing policies and various requirements may need to be met whether that be to adhere to the law such as paying taxes, or to adhere to ISO 27001 standards, one such action All n One as a company developed due to ISO 27001 was a handling of assets policy which included, the retrieval of stored assets, the ownership of the asset or the return of an asset. Another requirement might concern a higher level policy that ‘already exists in the organisation’ being considered (Kosutic [2], 2016).

### Risk Assessment

When developing the policies and procedures of a company it might be of help to take into account the results from the risk assessment previously done (Kosutic [2], 2016), which was indeed kept in mind when All n One were developing their policies and procedures. By doing so the documentation for the policy or procedure may outline potential risks within the operation to look out for or the steps involved may include steps to mitigate the potential risk.

### Optimization

When creating documentation for Policies and Procedures the organisation of said documents should be kept in mind, Mr Kosutic asks when considering organisation, ‘are you going to write ten 1-page documents or one 10-page document?’ (Kosutic [2], 2016) he goes on to mention that the management of one document would be easier than 10 separate documents especially when the target group of readers is the same.

All n One developed their policy and procedures in a way that each department have their own policies and procedures that affect them grouped as a single document. This provides the employees of each department the correct policies and procedures they need to conform to without the inclusion of non-relevant information.

To reduce redundancy within the policies and procedures if an issue is already covered within a different document a link to that document is put in place as well as a location to find the document.

### Structure of Documentation

ISO 27001 includes the implementation of ‘a procedure for document control’ as such All n One have developed a standard Template that all documentation is to equate to as well as a process the documentation goes through before approval.

### Approval

As for Approval itself when developing policies and procedures unless a senior manager or someone with the correct authority were to develop these policies or procedures the created documentation might not be enforceable meaning it may have to be approve by such a person before it can become a true policy or procedure (Kosutic [2], 2016).

This too had taken place within All n One where when creation of a policy or procedure the documentation was sent to the senior security manager for approval before the staff was required to adhere to it.

### Employee Awareness

It might be required to notify employees of changes within the workplace or rather explain to the ‘employees why such a policy or procedure is necessary – why it is good not only for the company, but also for themselves.’ (Kosutic [2], 2016).

Training of Employees may also be required to make sure everyone can adapt to the changes.

### Maintenance

Once the policy and procedures documentation have been completed continual maintenance of the documents is needed to keep them up to date and relevant similar to the continual audits of ISO27001 continual audits of policies and procedures to make sure they continue to ‘fill their purpose’ (Kosutic [2], 2016) and that best practice is always kept in mind.

# ISO 27001 Audits

To obtain ISO 27001 certification the company must go through two audits labelled stage one and stage two. There is also an additional audit that happens prior to the stage one and stage two called a gap audit.

## Gap Audit

All n One as a company had decided to conduct a gap audit. The gap audit consisted of a certified ISO auditor to advise All n One of the nonconformities that were present within the All n One infrastructure.

Nonconformities refer to requirements that have not been met (Kosutic [3], 2014) meaning that a standard that has been set had not been met (Kosutic [3], 2014). An example of nonconformity might be ‘If you don’t have records of corrective actions, and the standard requires you to have them’ (Kosutic [3], 2014).

## Stages

### Stage One

Stage one of the Audit process consists of a certified auditor coming to review documentation to make sure it is compliant to ISO 27001 standards. Stage one is also known as the ‘Documentation review’ (Kosutic [4], 2016).

### Stage Two

Is considered the main Audit and as such is more complex than simple document review. In stage two the certified auditor comes to check and see if the company is not only compliant with ISO 27001 but also with the organisations documentation. (Kosutic [4], 2016).

# Business Operations

This section is solely dedicated to outlining the effects that the ISO 27001 process has had on a business like All n One.

## Infrastructure

The process of ISO 27001 has changed the infrastructure within All n One in many ways. Due to it being a small company All n One had often seen the boundaries of departments bend or disappear at times to keep up with the influx of work.

With ISO 27001 however that is no longer the case. Department borders are now highlighted and enforced each employee has a department they are assigned to and will no longer partake in work outside of their departments.

## Organisation

From what has transpired throughout the process of ISO 27001 it can be noted this change to infrastructure and reinforcement is most likely due to the policies and procedures that have been put in place allowing employees to perform work at a quicker rate thanks to the set in policies and procedures, so guidance is constantly given and the opinion of senior level management is not needed as greatly.

## Business

All n One has seen an influx of business since campaigning for ISO 27001 and will possibly see an even bigger increase after certification. Reasons being that companies see that All n One is a company that is becoming even more secure than it already was and the peace of mind an ISO 27001 certified company offers is extremely beneficial to potential clients

# References

MSM (2015) ISO 27001 certification | IMSM Ltd. Available at: http://www.imsm.com/gb/iso-27001/?gclid=CI3NsMrFwMwCFQmK2wodsRcODQ (Accessed: 4 May 2016).

Advisera, E.S. (2016) What is ISO 27001? Available at: http://advisera.com/27001academy/what-is-iso-27001/ (Accessed: 10 May 2016).

Kosutic, D. (2016) ISO 27001 asset register: How to develop an asset inventory. Available at: http://advisera.com/27001academy/knowledgebase/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/ (Accessed: 12 May 2016).

Vigilant (2016) Vigilant software Blog. Available at: http://www.vigilantsoftware.co.uk/blog/conducting-an-asset-based-risk-assessment-in-iso-270012013/ (Accessed: 16 May 2016).

Jakeman. (2016), Risk Rating matrix [ONLINE]. Available at: http://www.jakeman.com.au/media/whats-right-with-risk-matrices [Accessed 20 May 2016].

Kloosterman, V. (2013) What are the 12 key elements of a project risk register template? Available at: http://continuingprofessionaldevelopment.org/key-elements-project-risk-register-template/ (Accessed: 20 May 2016).

Risk mitigation planning, implementation, and progress monitoring (2013) Available at: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring (Accessed: 21 May 2016).

Company policies and procedures (2011) Available at: http://www.pcg-services.com/resources/policies-procedures-barrier-growing-company/ (Accessed: 21 May 2016).

Kosutic [2], D. (2016) ISO standards: Seven steps for implementing policies & procedures. Available at: http://advisera.com/27001academy/knowledgebase/seven-steps-for-implementing-policies-and-procedures/ (Accessed: 21 May 2016).

Kosutic [3], D. (2014) ISO 27001 certification – major vs. Minor Nonconformities. Available at: http://advisera.com/27001academy/blog/2014/06/02/major-vs-minor-nonconformities-in-the-certification-audit/ (Accessed: 21 May 2016).

Kosutic [4], D. (2016) Becoming ISO 27001 certified – how to prepare for certification audit. Available at: http://advisera.com/27001academy/knowledgebase/becoming-iso-27001-certified-how-to-prepare-for-certification-audit/ (Accessed: 22 May 2016).