Platinum SQUARED

# Using Collaboration Tools to Achieve ISO 27001 Certification

How Collaboration Tools can aid in implementing an Information Security Management System

## Introduction

Platinum Squared (P2) is a small company specialising in the areas of information assurance and information security. The nature of P2's work makes it important that we are able to demonstrate to our existing and prospective customers that we can handle their information in a secure and responsible fashion.

The leading international information security standard is ISO 27001 - Information Security Management Systems which has a long history and is well understood and respected within the information assurance sector, and so we identified the need to achieve certification against that standard.

We are a lightly structured organisation, with each of our consultants largely responsible for organising their own work-load and even deciding on what information systems best suit their own particular needs. Our consultants work for a variety of clients and are typically based either on client's sites or regularly work from home. We do not have a conventional corporate network, nor a corporate file server. Instead we use a variety of cloud-based services accessed from our laptops.

Initially, it appeared that the lack of centralised IT systems within P2 would make the task of achieving ISO 27001 certification very difficult. However, we have been able to set up an Information Security Management System (ISMS) that allows us to fulfil the requirements of ISO 27001 in a systematic and thorough fashion and to put together a set of policies and a governance framework that meets P2's own requirements and has satisfied, even impressed, the independent ISO 27001 auditor who assessed P2's compliance against that standard.

The objective of this White Paper is to record some of our experiences of putting ourselves through the ISO 27001 certification process. It highlights the benefits that the process has brought to the company and how the various tools we have used or developed assisted in achieving the goal of being awarded ISO 27001 certification and continues to assist in running our ISMS.

## Reasons for aiming for ISO 27001

As a supplier providing services to many organisations who handle sensitive information including many Government Departments, public sector bodies or commercial companies, P2 is regularly required to confirm that it complies with ISO 27001 - Information Security Management Standard.

Even from an early stage in the company's existence, we implemented an Information Security Management System (ISMS) and a Security Improvement Programme that aimed to demonstrate compliance with the standard. However, we wanted to go a step further and achieve formal certification against ISO 27001. This certification was sought to:

- Give greater assurance to Government Departments, other customers, employees, trading partners and stakeholders that information security is being well managed within P2,
- Demonstrate our credibility and trustworthiness to these bodies,

- Achieve cost savings. Even a single information security breach can involve significant costs as well as reputational damage,
- Establish and demonstrate that relevant laws and regulations are being met,
- Help us demonstrate credibility when we are providing services around the certification against ISO 27001 to our clients,
- Demonstrate that an ongoing commitment to Information Security exists at all levels throughout the company.

## Issues facing P2 in achieving ISO 27001

We have a small office location near Bedford which provides a convenient location for company meetings or meetings with clients. However, all members of staff, including the Directors, are actively engaged in delivering consultancy services for our customers. As a result, our staff work in a wide variety of locations, including client sites and from their own homes. The demands on the consultants' time mean that it would be impractical to have regular face to face meetings with colleagues so the office in Bedford is used only on an occasional basis.

All members of P2 staff are equipped with laptops and mobile phones to enable them to carry out their work, but we do not have its own network or servers or any other centralised IT functions that would normally be expected in a larger organisation. Even the laptops and phones can vary from consultant to consultant because we provide the flexibility to choose what sort of device fits best with their experience and their preference on what would enable them to support our clients most effectively.

This means that when our ISO 27001 project commenced there was a wide variety of approaches taken to securing the information that we handle and only limited guidance issued on what was considered good practice.

What we wanted to achieve was a consistency of approach but without forcing people adopt a single solution which might damage the consultants' ability to deliver their work in the most effective manner for our clients. Central to achieving that objective was the use of a variety of collaboration tools.

## Collaboration Tools in use

A 'Collaboration Tool' is defined as:

> A technology tool that can be used to help people work together to achieve a common goal or objective.

Such tools are often delivered as internet or cloud-based services and can provide a range of services including:

- Document storage and management,
- Project Management,
- Task Management,
- Time recording,
- Customer Relationship Management,
- Communications (including phone calls, video calls, conference calls),
- Accounting.

The distributed nature of our staff means that it really benefits from using such tools. The specific tools that we use are shown below:

- Box Document Management (https://www.box.com/en-gb/home),
- Skype (https://www.skype.com/en/new/),
- Microsoft Office 365 (https://www.office.com/).

This White Paper is **not** saying that it is essential to use these tools or even recommending that these particular tools are the best ones to use. Rather it is illustrating what is possible with collaboration tools by showing examples based on these packages.

**Setting Up the ISO 27001 Project**
For an organisation to achieve ISO 27001 it is necessary to set up a team who are clearly focused on conducting the activities necessary. For us, this involved:

- Setting up the P2 Security Working Group (SWG), which sets the general direction for the company and ensures that there is agreement by all stakeholders on important elements of security strategy.
- Setting up the P2 Security Working Party (SWP), which is responsible for items such as conducting the risk assessment, preparing and reviewing the policies and achieving and maintaining certification.

Given the small size of the company, the SWG is generally attended by all of the P2 Directors and most of our employees. It is normally held in conjunction with our company meetings and provides an opportunity to keep everyone up to date with the changes in policy, progress on the ISO 27001 certification project, deliver training and reinforce messages about the need to maintain security.

Most of the work on producing, reviewing and issuing the risk assessment and the supporting policies was conducted by the SWP. The SWP would meet once every 2 weeks using Skype to review progress on the tasks that had been identified from various sources.

## Setting the scope and timetable

Setting the scope of the ISMS is critical to both achieving a successful certification against ISO 27001 and also satisfying our customers that their information is properly protected.

We aimed to set a scope that covered all of our consultancy services and the IT facilities used to provide those services. As required by ISO 27001, we also prepared a scope document setting out the details of those services and the IT facilities, which included the collaboration tools that we use to deliver our consultancy services. Since these collaboration tools are based in the Internet and used by multiple organisations, we needed strong assurances from each supplier about how they enforce the required levels of confidentiality, integrity and availability, and ensure the separation of our data from other customers.

Collaboration tools were particularly helpful when conducting the Risk Assessment and working on the implementation project, supporting the Security Working Group meetings and the on-going compliance audits that we set up.

## Setting up the Security Working Group and Security Working Party

As part of setting of the Information Security Management System (ISMS), we set up the P2 Security Working Group (SWG) which provided an opportunity for all stakeholders to see the key documents and agree the important decisions that were being taken as part of running the ISMS. However, this was too large a group of people to get together on a regular basis, so we also set up a smaller Security Working Party (SWP) consisting of 3 or 4 people. These people were those individuals most actively involved in writing the policies that were needed or conducting the risk assessment and the on-going compliance audits.

The SWG would meet only once every 2 or 3 months, but the SWP was set up so that it would take place once every 2 weeks and it was deliberately limited so that it would only last 1 hour. Experience showed that if the meetings are longer they tend to lead to people using the opportunity to discuss issues that were not relevant to pushing the ISO 27001 project forward. By limiting the time to just an hour, it meant that everyone had to focus on the outstanding actions that needed to be completed if we were to complete the project in the time that had been allotted. The SWP was led by one of the P2 Directors which demonstrated senior management interest and focus on activities that were being taken. It also meant that, where necessary, quick decisions could be taken within the meetings, without having to wait for confirmation from the formal Security Working Group.

**Collaboration Tools Used**

**Use of Box**
Since our staff work in a range of locations, we needed a centralised place for storing the documents that we create or work on collaboratively which could be accessed over the Internet in a secure manner. The software also had to allow our staff to synchronise the files in their folders to their laptops so that they could continue to work even when there was no internet connection available.

We selected the Box document management system because it met these essential requirements and it also provided a range of other features, such as flexible access control and auditing capability, that proved to be extremely valuable when developing the documentation required to achieve ISO 27001 certification.

**Use of Skype**
Skype provides voice, video conferencing and instant messaging facilities. The main use that we made of Skype was its ability to hold multi-party calls. We held a virtual Security Working Party meeting once every two weeks. These calls were set up by the Director leading the ISO 27001 project and were normally attended by the 3 or 4 people who were most involved in carrying out the actions.

Skype also provides the facility for participants in the group call to share their desktop, i.e. allow other people on the call see an image of the screen that the participant is working looking at. This enabled the host of the Security Working Party to show the various actions lists that have been used to drive the work on compliance against ISO 27001.

**Use of Office 365 and Excel**
Microsoft Office is a widely used suite of Office Productivity tools. Of these applications, the most relevant to achieving ISO 27001 certification for us was Microsoft Excel. We used Excel to:

- Document the risk assessment,
- Record the status of all the policies and procedures that we wanted to produce
- Prepare self-assessment questionnaires in support of compliance audits on topics such as home-working and use of laptops,
- Maintain the action lists to address any remedial actions noted in any of the above activities.

We even used Excel to prepare a ‘pop quiz’ questionnaire which was used to test people’s basic understanding of security terms and be part of our security awareness campaign.

Given the technical background of members of the SWP, we have a fair amount of experience of macros and VBA within Excel. We have used that experience to develop several functions which can help in creating and maintaining these spreadsheets.

Platinum SQUARED

## Building the Information Security Management System (ISMS)

### Creating Policy Structure

An essential element in running an Information Security Management System is having a set of appropriate documentation to define:

- The company's policies and objectives;
- People's responsibilities in following those policies;
- The detailed procedures that people need to follow to adhere to the policies.

In order to identify the security documents we required and the status of that documentation, we prepared an Excel spreadsheet which showed the typical documents that an organisation might have, how these related to the ISO 27001 controls and then what was our local equivalent document. This enabled us to identify if there were any additional documents that we needed to prepare and make sure there was adequate coverage for all the aspects of security.

We used the spreadsheet to record:

- The name of the policy and notes about the policy,
- The current version and the date it was published,
- A hyperlink to the document itself,
- The owner of the policy,
- The date that it is scheduled to be reviewed,
- Cross references to any actions associated with that policy,
- Cross references to the ISO 27001 controls that the particular policy addresses.

When preparing the documentation there will always be occasions when further actions are needed. One of the principle mechanisms that we used to ensure that these deficiencies were addressed was to include an Actions worksheet in this (and other spreadsheets) which allow us to record the nature of the deficiency and whose responsibility it was to fix the problem.

The list of actions from this spreadsheet was one of the standing items on the agenda for the Security Working Party. At each meeting we check to see if any document needs to be reviewed or re-issued and then we go through all the open actions to see the progress that has been made in completing those actions.

In addition to the actions recorded in the List of Policies and Procedures spreadsheet, much of the detailed discussion about the contents of specific policies is captured using the comments facility provided by Box.

Using Box it is possible to add comments into a document which can then be seen by the other collaborators on the document. It is possible to turn these comments into tasks so that the author of a document can task a collaborator to review / update a particular document or section.

We found this facility to be particularly useful when formally issuing a policy because a task can be assigned to all recipients of the policy to confirm that they have read, understood and agree to abide by it. Using this facility, we have been able to track who has and who has not signed up the relevant policies.

### Defining Roles and Responsibilities

As set out in the ISO 27001 control A.6.1.1 – Information security roles and responsibilities:
All information security responsibilities shall be defined and allocated.

This is just as important in a small organisation as it is in a large organisation even if several roles may be fulfilled by the same individual. We prepared a Roles and Responsibilities document which set out a total of 16 roles. Defining a consistent set of roles at the start of the ISO 27001 project meant that we could be clear about who was responsible each area and we could provide the evidence necessary about how security responsibilities had been divided up.

It is worth noting that we defined more roles than people in the company! However, this enables us to move particular responsibilities between people as the company changes without having to revise our security policies.

**Conducting Risk Assessment**

As a company we have extensive experience in not only conducting risk assessments but also in developing risk assessment methods and the tools to support those methods.

Using this experience, we have developed a spreadsheet-based approach to risk assessment that we call RiskSafe Assessment. This method has been developed to assist in completing some consultancy assignments for our clients and to meet ISO 27001 requirements elsewhere.

RiskSafe was developed to assist with the following tasks:

- Undertaking a risk analysis of information systems and networks,
- Identifying security requirements and possible solutions,
- Recording the evidence that measures are in place or the remedial actions required to fix any weaknesses observed.

The spreadsheet consists of the following worksheets:

- Version control,
- Introduction,
- Asset summary,
- Detailed Business Impact Assessment (BIA) for each information asset,
- Threat and vulnerability assessments for each part of the risk assessment,
- Guidance on Impacts that the threats may cause,
- Risk matrix,
- Guidance on countermeasures that may help address the threats that have been identified,
- Guidance on ISO 27001 controls that may help address the threats that have been identified,
- The ISO 27001 Statement of Applicability (SoA),
- A copy of the policy and procedures worksheet,
- The actions identified when completing the ISO 27001 Statement of Applicability and other parts of the risk assessment,
- Audit log of updates to the risk assessment.

The most important of these worksheets is the one recording the information about the ISO 27001 controls. This worksheet acts as our Statement of Applicability, but it also provides the way of:

- Recording the current status of each of the ISO 27001 controls,
- Identifying which policies helped support the implementation of that control,
- Cross-referenced to any remedial actions needed to address weaknesses identified,
- Acted as our Risk Treatment plan by showing which of the risks identified in the risk assessment were addressed by each of the controls.

The most important aspect of running an Information Security Management System (ISMS) is the concept of continual improvement. Central to this concept is the need to identify areas where weaknesses either exist or there are opportunities to improve current ways of working.

In order to support this assessment, the Risk Assessment spreadsheet contains a function that allows us to create and maintain any actions that we identify during the course of conducting the risk assessment. This work helps populate the Actions worksheet, which is similar to the Actions worksheet in the List of Policies and Procedures spreadsheet. As noted previously, once every 2 weeks the SWP would review the open actions on this Actions list to ensure that remedial actions were being followed up.

**Conducting Compliance Audits**

In order to demonstrate that our policies were not simply 'paperware', we needed to put in place a Compliance Audit programme.

We drew up an audit schedule which enabled us to set out a set of audits that ensured that we covered all the relevant ISO 27001 controls in a structured timescale, and we divided each of those audits between the members of the SWP.

Most audits followed a set pattern of reviewing the existing policy documentation and then having an interview with the person or people responsible for implementing those policies. A formal audit report would be prepared which set out any non-conformities or observations and this audit report could be discussed at both the SWP and SWG meetings.

The exceptions to this method of working were the audits on our home working policy and laptop policies. In these cases, we prepared a questionnaire which set out the requirements detailed in these policies and copies of these questionnaires were distributed to all members of staff for completion.

All non-conformities from any of these audits are recorded in the SWG Action list and then monitored as part of the regular work of the SWP.

**Conducting the ISO 27001 Certification Audit**

We contracted Exova (https://www.exovabmtrada.com/en-gb) to conduct our ISO 27001 certification audit. In preparation for that audit we discussed and agreed what documentation should be made available to our auditor. In summary this included:

- P2 Information Security Policy,
- Roles and Responsibility document,
- Security Management Framework document,
- Terms of Reference for the SWG,
- Risk Assessment spreadsheet,
- Statement of Applicability,
- Business Impact Assessment reports,
- Copies of internal audit reports and external audit reports, such as our Cyber Essentials Plus certification.

We created a Stage 1 Evidence Folder which included copies of all of the above information and using Box's collaboration facilities we were able to make that folder available to the Auditor, so that she could conduct her documentation review prior to conducting the Stage 1 audit.

Having explained how these documents had been created and were being maintained in the stage 1 audit, the auditor asked for supplementary evidence in a few areas, which we were able to provide in a similar shared folder prior to the stage 2 audit.

We were awarded ISO 27001 certification on 6 February 2018.

**Maintaining Policies and Procedures**
We fully appreciate that achieving ISO 27001 certification is not a one-off exercise, where it would be acceptable to reduce the attention that is being paid to information security once certification is achieved.

We are continuing to run the SWP meetings on a regular basis following exactly the same format as we followed in the run up to ISO 27001 certification.

In summary, this means that each meeting we:

- Review the list of policies and procedures to determine which of those are approaching their review dates, and set actions for someone to conduct those reviews,
- Review any outstanding actions from the reviews that have been carried out on those policies and procedures,
- Review the compliance schedule and any compliance audits that have been conducted since the last meeting,
- Review any outstanding actions from previous audits,
- Reviewing any changes to the business that may require changes to policies, procedures or the risk assessment.

**Conclusions and Lessons Learnt**
When we started on the ISO 27001 project, it appeared a daunting task because we are such a diverse organisation working in many locations and using a wide variety of IT systems.
However, the process of working collaboratively in pulling together a set of policies and procedures which meet all of our needs provide opportunities for people to share experiences and increased the feeling that people were working as part of a team.

The use of the collaboration tools was essential in completing this work but also demonstrated that these tools can provide new ways of working which are more flexible and have increased efficiency. These lessons can be applied to many other projects and how, when used properly, organisations can make significant savings in terms of monitoring and controlling those projects.

Achieving ISO 27001 certification has improved our security policies and gives all of us a greater degree of confidence that we can demonstrate that we are handling our and our client's information in an appropriately secure manner, but rather than being seen as a burden or an administrative overhead, the processes of working together increased our sense of working together for a common goal.

## About the Author

Jonathan Tregear is a leading figure in the areas of risk analysis and risk management, and has lectured widely on these topics, both within the UK and internationally. He is considered to be one the most experienced risk analysts in the country and was responsible for the design and development of two risk assessment methods, namely CRAMM and RiskSafe Assessment.