Customer	**:**	**Platinum Squared**	**Document Ref**	**:**	**41059-3-1**
Contract No	**:**		**Issue Date**	**:**	**13/11/2019**
WP No	**:**		**Issue**	**:**	**1.0**

Title : **P2 White Paper – Using ISMS On-Line to help achieve ISO 27001**

Abstract : The objective of this report is to provide a case study on how ISMS On-Line can assist organisations in implementing an Information Security Management System and thereby achieving certification against ISO 27001

Author : Jonathan Tregear

Approval :

Accepted :

Distribution :

Hard Copy File:
Filename: Using ISMS On-Line to achieve ISO 27001 (v1.0)

TABLE OF CONTENTS

AMENDMENT POLICY

This document shall be amended by releasing a new edition of the document in its entirety. The Amendment Record Sheet below records the history and issue status of this document.

AMENDMENT RECORD SHEET

ISSUE	DATE	REASON
0.1	14 August 2019	Initial draft
0.2	19 August 2019	Issued for internal review
0.3	3 September 2019	Issued to Alliantist for review
1.0	13 Nov 2019	Published

1. INTRODUCTION

1.1 Purpose and Scope

Platinum Squared (P2) are small group of consultants who are specialists in information assurance and information security working with a range of clients in the public and private sectors.

The nature of P2's work makes it important that we are able to demonstrate to existing and prospective customers that we can handle their information in a secure and responsible fashion. The leading international information security standard is ISO 27001:2013 - Information Security Management Systems which has a long history and is well understood and respected within the information assurance sector. As a result, P2 decided to seek certification against this standard, which we achieved in October 2017.

A key aspect of running our Information Security Management System (ISMS) is use of the cloud-based service, ISMS On-line. This service fits in well with our approach to using cloud-based services to run our business, providing us with the high degree of flexibility that we require.

The objective of this White Paper is to record some of P2's experiences of putting ourselves through the ISO 27001 certification process and how ISMS On-line has helped us in maintaining that certification and running our ISMS, as well as making some suggestions how ISMS On-line can be extended to provide support in other areas.

2. BACKGROUND

2.1 Overview of Platinum Squared

P2 provides consultancy advice in the following areas:

- ISO 27001,
- Risk Assessment,
- Legal Compliance and Data Privacy,
- Information Security Policies and Procedures,
- Technical Security.

Our client base includes:

- Numerous Government Departments and Agencies,
- Public sector organisations including County Councils, various Police Forces and Health Authorities,
- Service Providers,
- Financial Sector organisations including various Banks and Building Societies.

We currently employ 9 people, including 3 Directors who also work directly as consultants. For most of the time, P2's members of staff are either based on client sites or are working from home. We do not have a wide or local area network, nor do we own or operate our own file servers or similar centralised IT systems. Instead we rely on facilities which are largely based in the 'cloud' and our laptops to access them.

2.2 Reasons for aiming for ISO 27001

As a supplier providing services to many organisations handling sensitive information including several Government Departments, Public sector bodies or commercial companies who are supporting Government Departments, P2 is regularly required to confirm that it complies with ISO 27001:2013 - Information Security Management Systems

Even from an early stage in its existence, Platinum Squared implemented an Information Security Management System (ISMS) and a Security Improvement Programme that aimed to demonstrate compliance with that 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 Platinum Squared,
- Demonstrate P2's 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 a commitment to Information Security exists at all levels throughout the organisation.

Over 80% of the consultancy business conducted by P2 in the last few years has either been delivered directly to public sector organisations or to commercial companies who are

themselves delivering services to public sector organisations. It is therefore important to take into account the types of policies and requirements that these public-sector organisations are obliged to follow.

2.3 Overview of ISMS On-Line

ISMS On-line (https://www.isms.online/) is a cloud based project management system which is specifically designed to assist in achieving ISO 27001 compliance/certification. It provides the following features:

- Policy creation, management and governance
- Information asset inventory
- Risk management & other decision support tools
- Statement of applicability for ISO 27001
- Incident management
- Staff and supplier compliance 'Policy Packs'

It comes with several in built 'projects' that are specifically designed to assist in implementing ISO 27001. It also supports the creation of 'trackers' which are lists of items, such as policy documents or corrective actions, that need to be reviewed on a regular basis to ensure that those items are being followed or maintained. ISMS On-line makes it easy to link items from one project or tracker to another project or tracker within the instance of ISMS On-line significantly simplifying the maintenance of the relevant information.

ISMS On-Line provides a project that lists all of the ISO 27001 clauses and controls to provide a basis for constructing a Statement of Applicability (SoA). It provides guidance on what type of information needs to be recorded against each of these clauses and control, including pre-written customisable text for most of the controls. This reduces the amount of time it takes for an organisation to prepare the SoA

The ability to link the items together means that this analysis can be linked to:

- Corrective Actions/Things to do
- Risk Assessments
- Stakeholder Analysis
- Internal and External documents
- Key Performance Indicators
- Policy Packs

As discussed in Section 0, the flexibility in ISMS On-Line means that it is possible to set up further projects / trackers to support other management standards such as:

- ISO 9001 (Quality Management)
- ISO 22301 (Business Continuity Management)
- Data Protection and GDPR

3. HOW ISMS ON-LINE HELPED MAINTAIN ISO 27001 CERTIFICATION

3.1 ISMS On-Line Projects and Trackers

ISMS On-Line has a number of in-built:

- Projects i.e. hierarchical structured area which are divided into:
  - Phases
  - Deliverables
  - Activities
- Tracks i.e. lists of items which typically have an associated status needing to be tracked

In addition, ISMS On-Line provides tools to help in tasks such as:

- Conducting the Risk Assessment (See Section 3.4)
- Issuing sets of documents that users need to read (See Section 3.9)
- Defining and monitoring Key Performance Indicators (See Section 3.10)

Amongst the in-built projects within ISMS On-line are ones that help with:

- Recording compliance against ISO 27001 (See Section 3.2)
- Conducting ISO 27001 Audits
- Running an ISMS Board
- Demonstrating compliance with GDPR

Amongst the tracks that ISMS On-line provides you with are:

- ISO 27001 Corrective Actions (See Section 3.6)
- Security Incident Management
- Information Asset Inventory

One of the major attractions of ISMS On-line is the ability it provides us with to create our own Projects/Tracks to supplement the existing in-built projects/tracks.

As described in the sections below, we created further projects/tracks to help in:

- Recording P2's Policies and Procedures (See Section 3.3)
- Setting out the results of the Business Impact Assessment conducted during the Risk Assessment (See Section 3.5)
- Recording Requests for Change (See Section 3.7)

3.2 Recording the Statement of Applicability (SoA)

The key project within ISMS On-Line with respect to achieving compliance or certification against ISO 27001 is the ISO 27001 project. This project allows organisations to record:

- Compliance against ISO 27001 Controls
- Cross references to evidence of compliance
- Details of any remedial actions required to achieve / maintain compliance and drive continual improvement
- Cross-refences to related risks

It supports the structure of the clauses and controls set out in ISO 27001 as shown below:

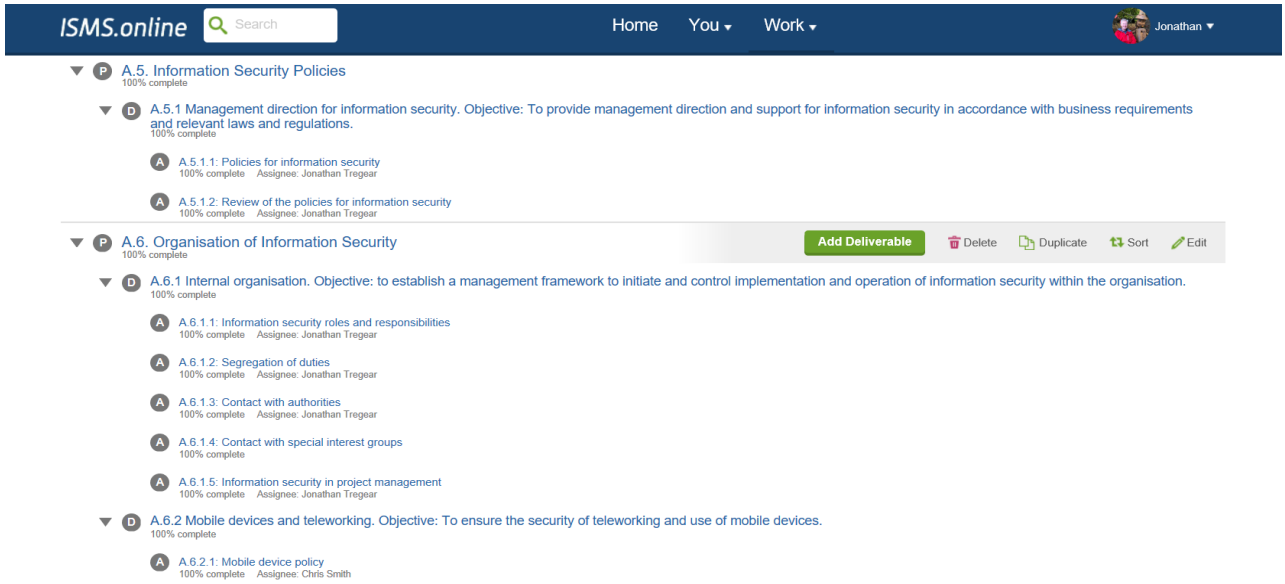


Figure 1 – ISO 27001 Project Structure

By selecting an individual control, it is possible to view or update the detail related to that control as shown below:

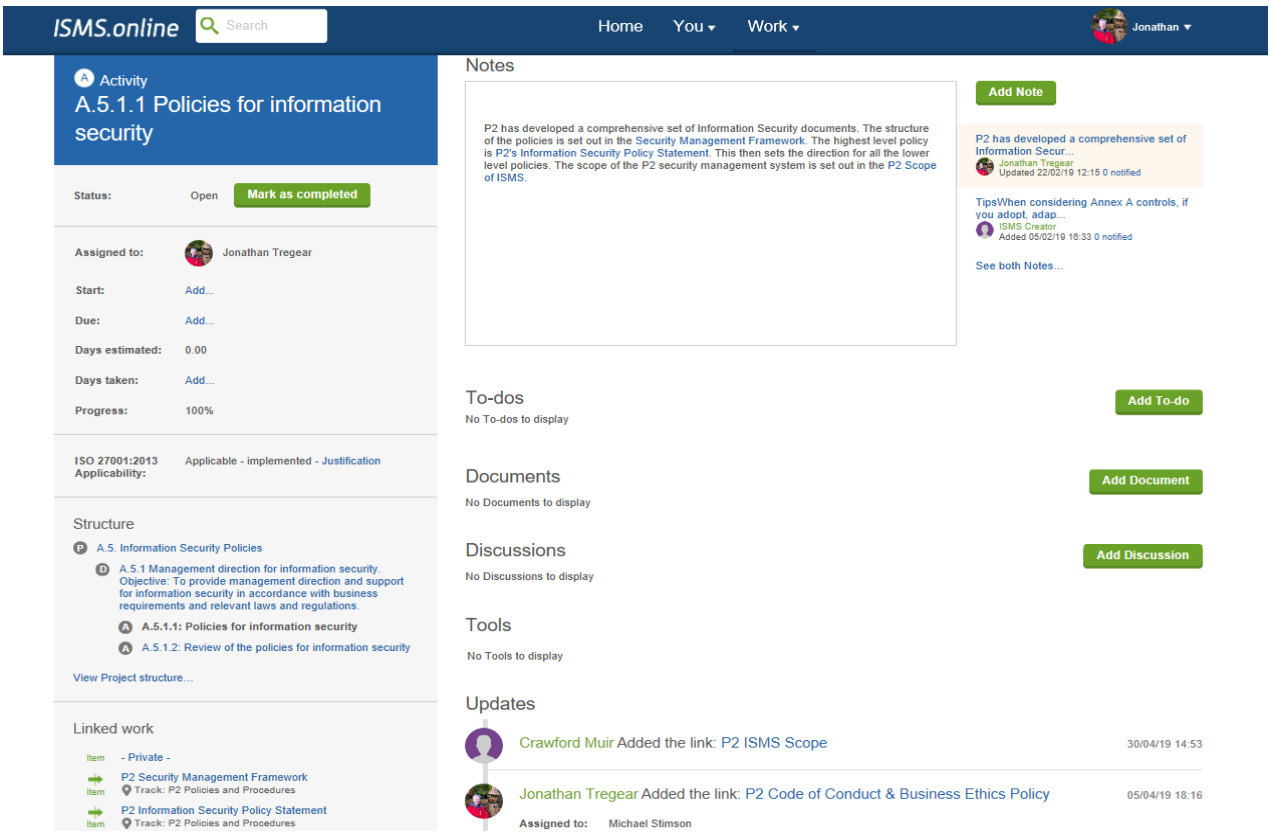


Figure 2 – Details of ISO 27001 Control

This screen allows us to record:

- Notes about how the control is implemented,
- The name of the person responsible for maintaining the control,
- The status of the control (in terms of percentage complete),
- Links to evidence about how the control is implemented (See Section 3.3 for more details about how policies and procedures are tracked)
- Links to the risk assessment (See Section 3.4 for further details)
- Links to corrective actions (See Section 3.6 for further details)
- Details of discussions related to the implementation of the control.

3.3 Tracking Policies and Procedures

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 in order to adhere to the policies.

In order identify what documentation we required and the status of the documentation we prepared a Tracker which set out all of P2's documents, as shown below:

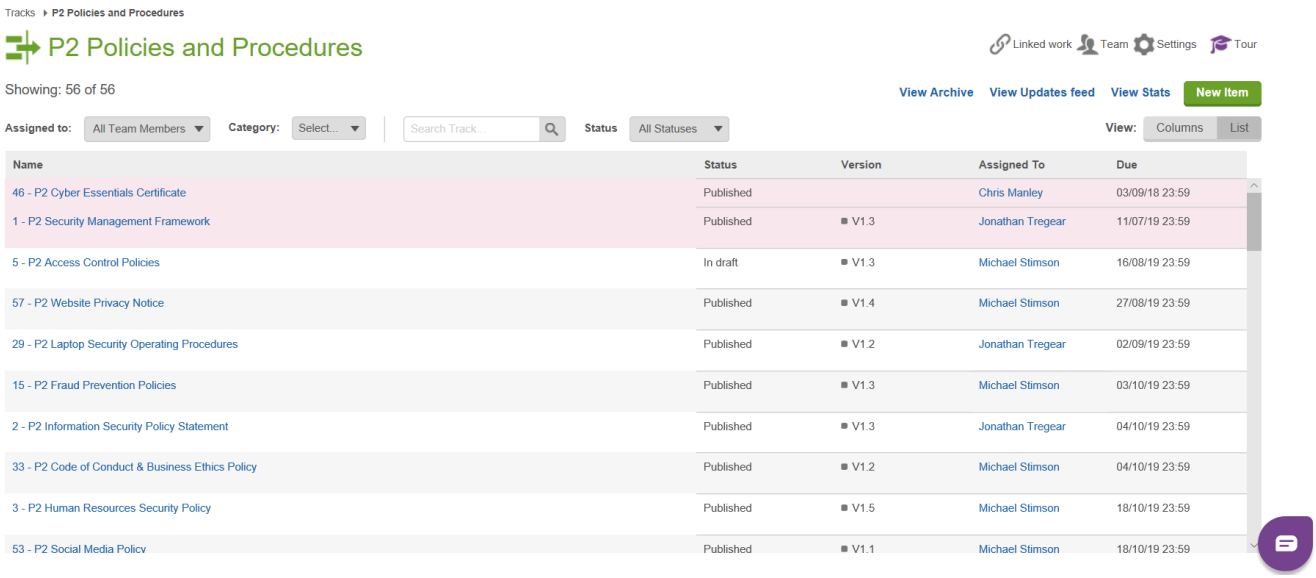


Figure 3 - P2 Policies and Procedures Tracker

By clicking on a document, we can see and record further details about the individual documents as shown below:

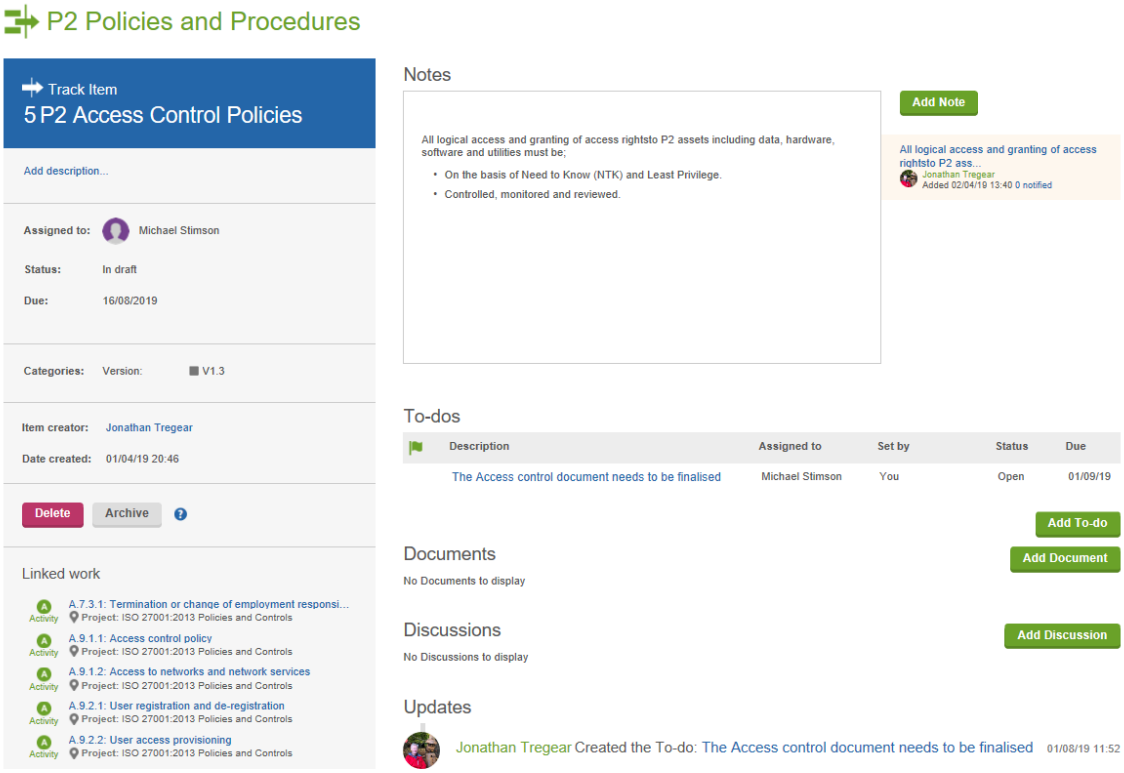


Figure 4 - P2 Policies and Procedures Tracker (Detail)

We use the tracker to record:

- The name of the policy or procedure and notes about the document,
- The current version and the date when the document needs to be reviewed,
- A hyperlink to the document itself (so the document does not need to be stored in ISMS On-line),
- The owner of the document,
- Details of any actions associated with that policy or procedure,
- Cross references to the ISO 27001 controls that the particular policy or procedure addresses.

Building this tracker has enabled us to have a clearly defined central list showing all of our policies and procedures, the links from these policies and procedures to how they support the ISO 27001 controls. Since the items use a hyperlink to reference where the documents can be found, it was not necessary to change the location of any of our documents, and the existing access control mechanisms means that those documents are only accessible to those people authorised to see them.

3.4 Conducting a Risk Assessment

Within the ISO 27001 Control project, ISMS On-line provides a Risk Assessment tool which allows you to record the threats that are relevant to your environment, and your assessment of them.

The following image shows the Risk Map view.

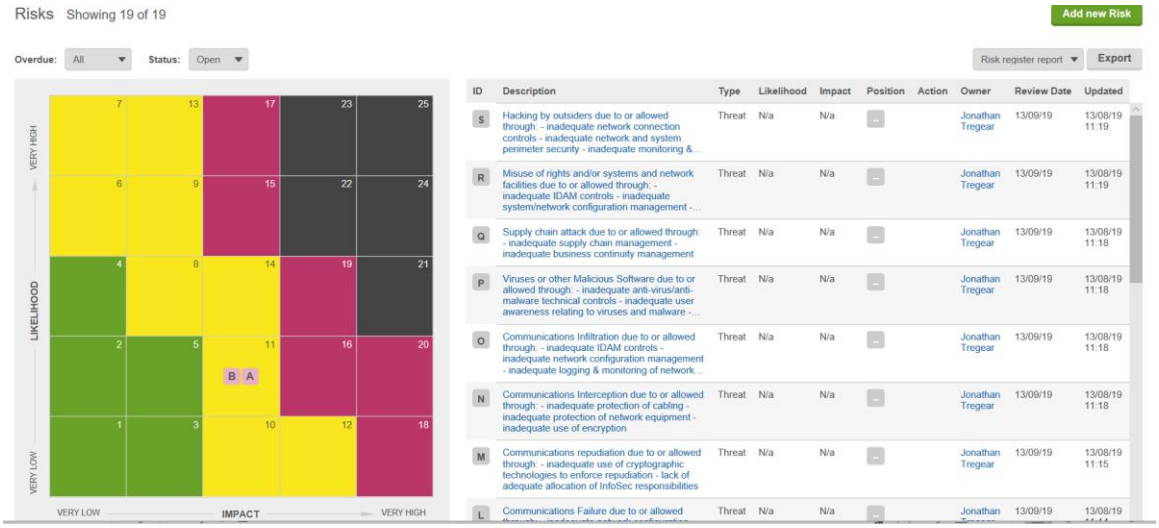


Figure 5 – Risk Map

A useful feature that ISMS On-line includes is a 'Risk Bank' of generic threats which organisations can select from to chose which are most relevant to their environment. This Risk Bank can significantly reduce the amount of time required to conduct the risk assessment.

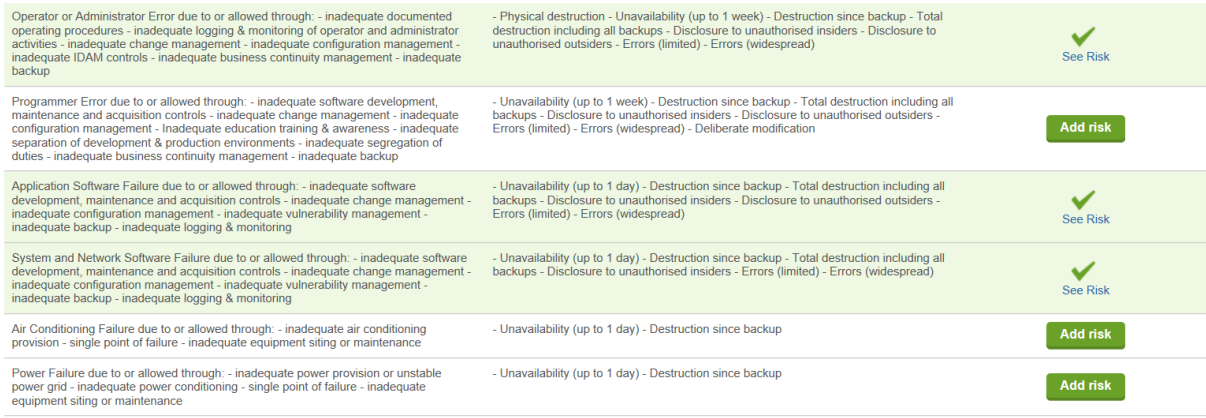


Figure 6 – Risk Bank

Having selected the relevant threats, you can use the following screen to record your assessment of the threat and the degree to which it is treated.

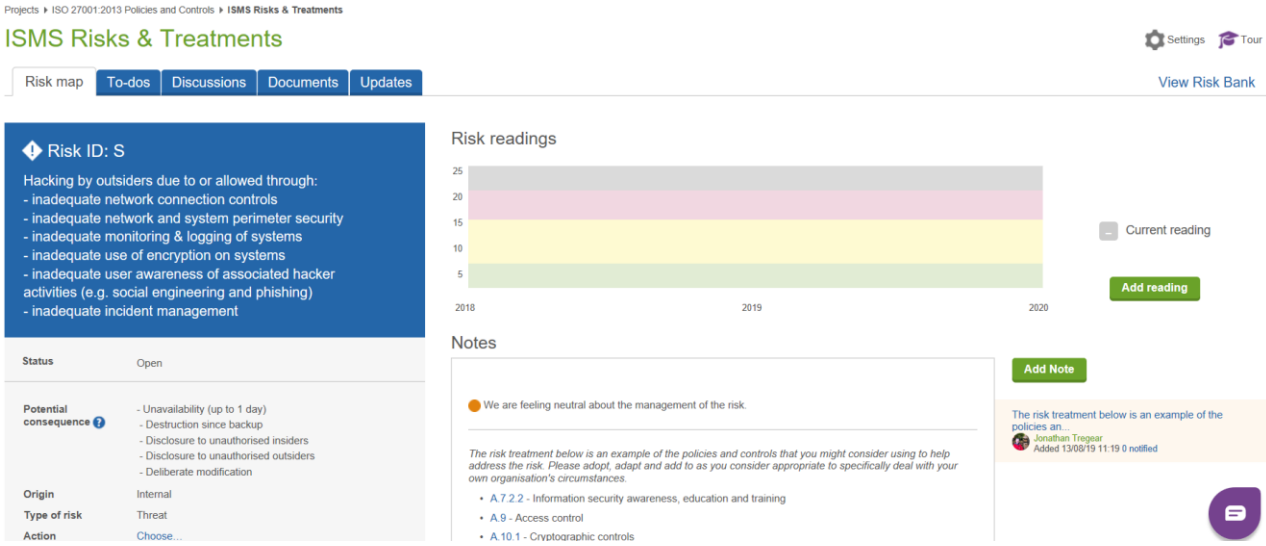


Figure 7 – Recording Risk Assessment

The threat can then be linked to the specific controls that help counter that risk.

If you used the Risk Bank option, ISMS On-line usefully provides a list of suggested controls that may help protect against those threats which can be easily linked to the risk assessment.

ISMS On-line then allows you to record the current assessments of threat levels and potential impact, together with the target levels for those assessments.

3.5 Business Impact Assessments

A key aspect of conducting a Risk Assessment is to complete a Business Impact Assessment. At the heart of information security are the requirements for:

- Confidentiality
- Integrity
- Availability

The objective of a Business Impact Assessment is to provide a systematic process by which an organisation can 'value' its information's requirements for these three attributes.

The Business Impact Assessment needs to gather and analyse information about an organisation's business functions and processes (applications, data) and the assets that support those functions (networks, information systems, facilities, people, places). It is important to recognise that Business Impact Assessments are essential elements in both Information Security Management and Business Continuity Planning.

P2 has extensive experience in conducting such assessments and has used that experience in documenting a series of valuation guidelines to allow the assessments to be conducted in a systematic and consistent fashion.

We created a tracker within ISMS On-line to record the results of the Business Impact Assessments that we conducted on the business services within our organisation.

The following image shows the list of business services that are included within the scope of our ISMS and the impacts associated with those business services.

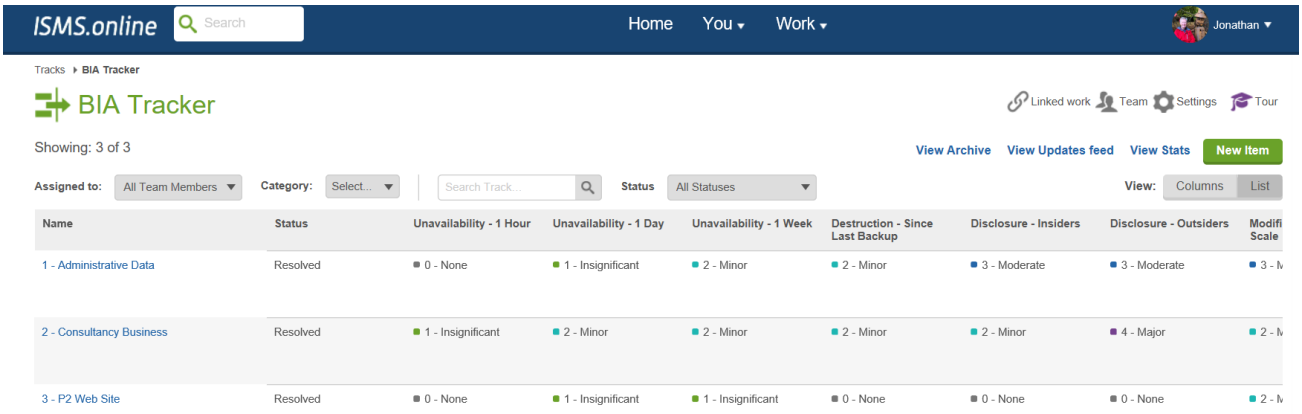


Figure 8 – Business Impact Assessment Tracker

The following figure shows how those assessments can be recorded/updated

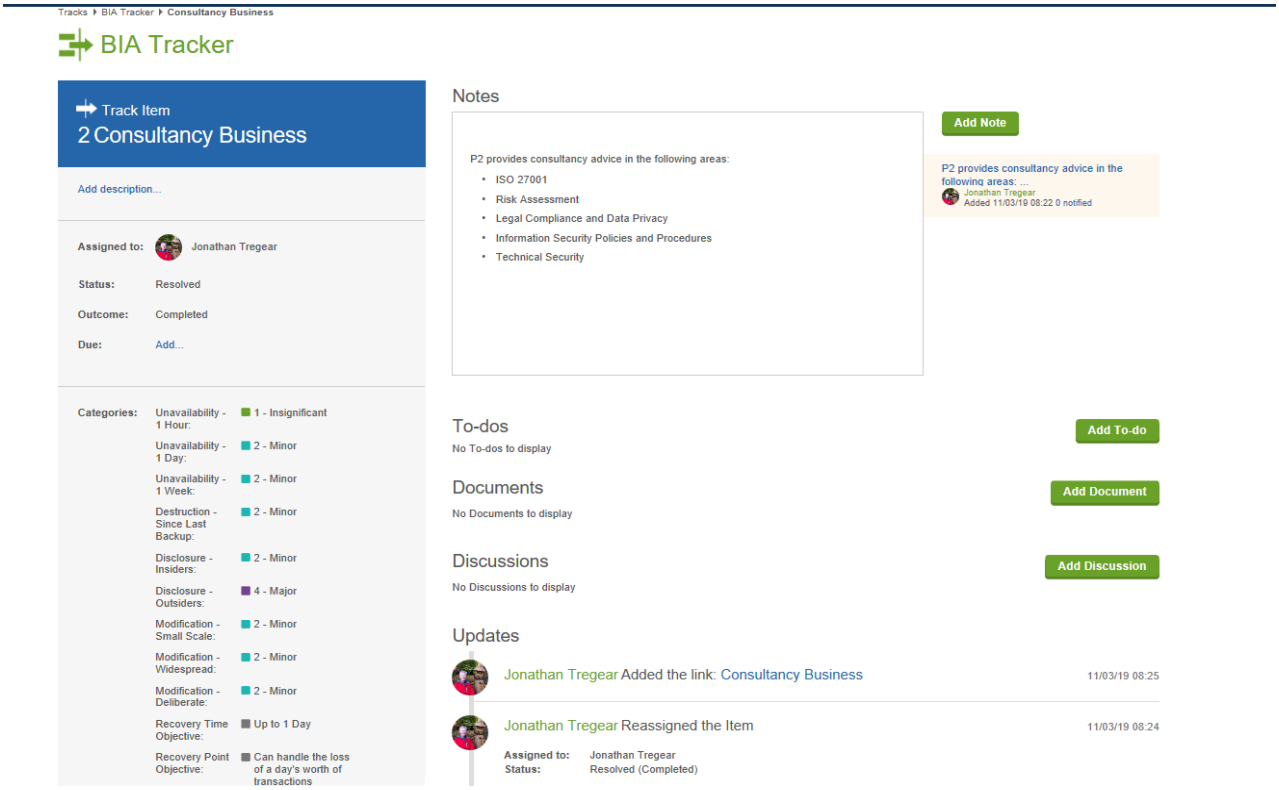


Figure 9 – Recording Business Impact Assessment

As can be seen from the above figure, it is possible to record the potential impacts from:

- Unavailability of the information
- Destruction of the information
- Disclosure of the information
- Modification of the information

In addition, the same tracker can be used to record the information's:

- Recovery Time Objective (RTO)

- Recovery Point Objectives (RPO)

The information about the consequences of unavailability of information and the RTO and RPO requirements are valuable information to include in the organisation's business continuity plans.

If required, the individual records can then be linked to more detailed records of the reasoning behind the impact scores. This can be set out in a document or, if you want, it is possible to create a project within ISMS On-line to record that information as shown below:

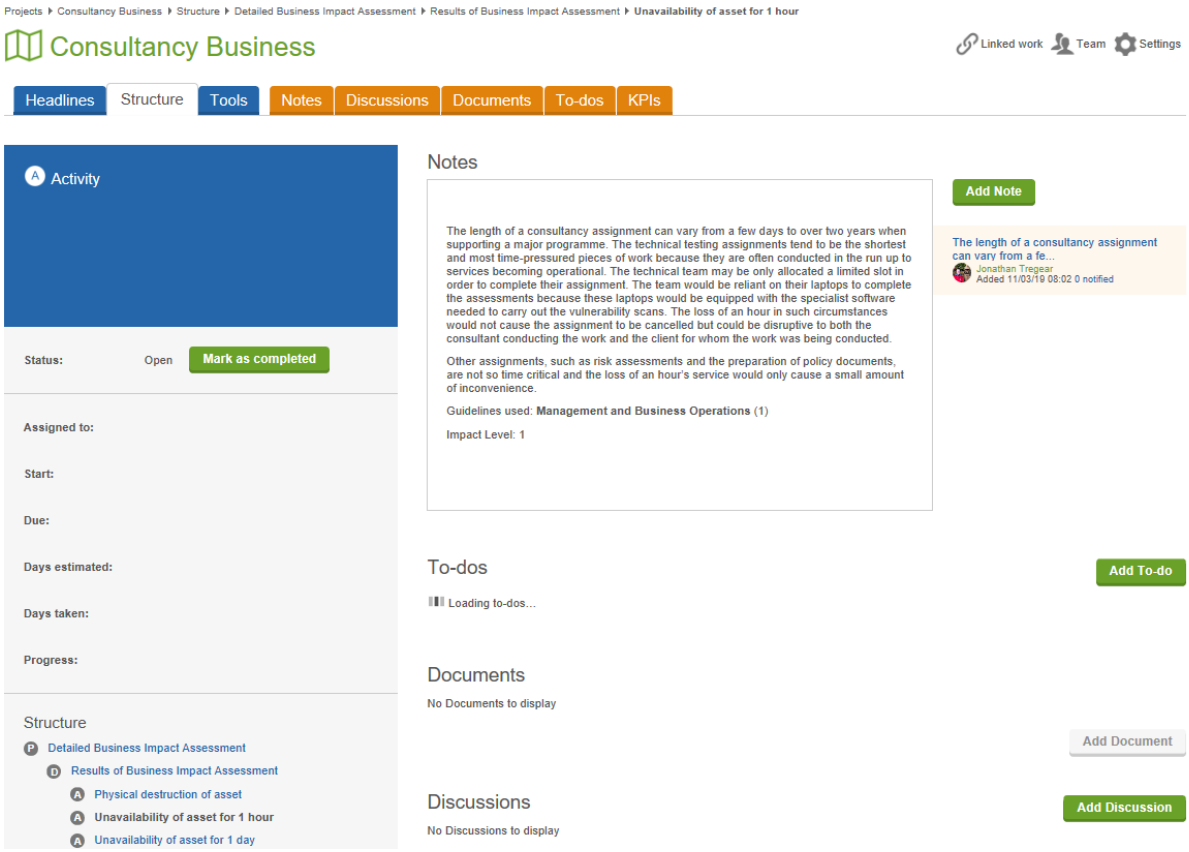


Figure 10 – Detailed Business Impact Assessment

3.6 Recording and Monitoring Corrective Actions

A key element to running an ISMS is maintaining on-going process for identifying, recording, monitoring and resolving any corrective actions.

ISMS On-line provides a Tracker which allows us to maintain a record on all the actions that need to be completed. The following diagram shows a snapshot of some of the actions that we raised whilst running our ISMS:

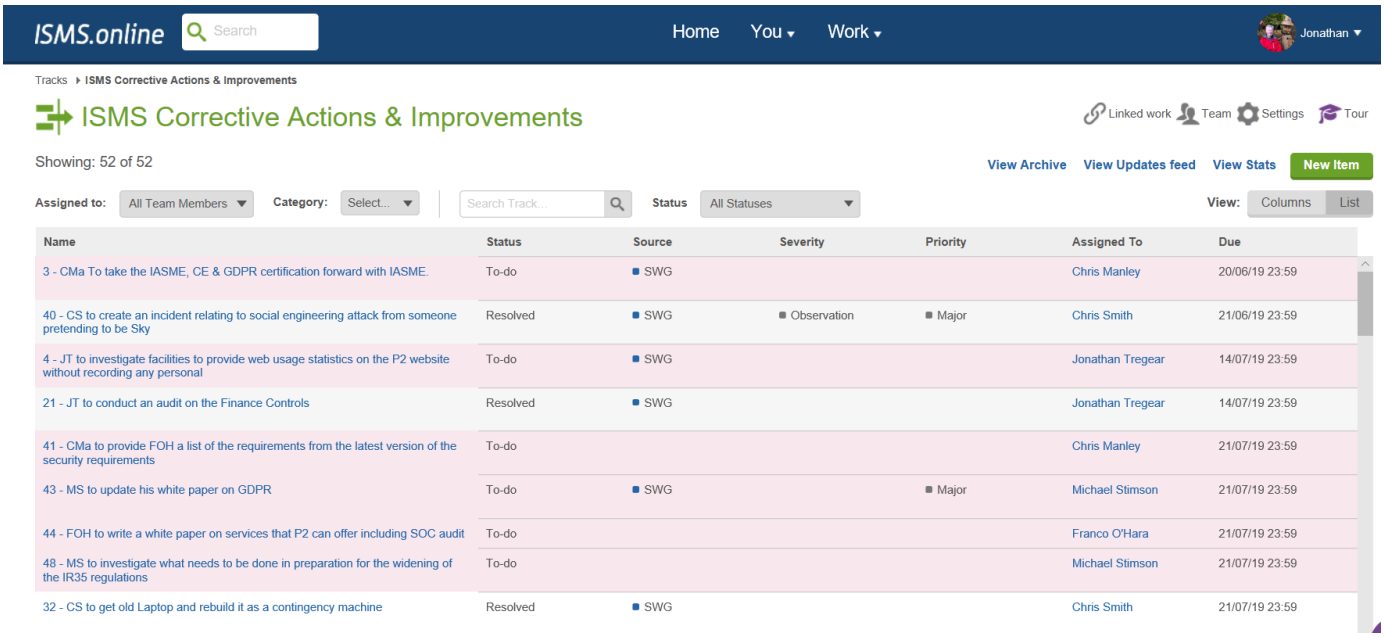


Figure 11 – Corrective Actions Tracker

Each of these actions can be expanded as shown in the following figure which shows the details of one of these corrective actions:

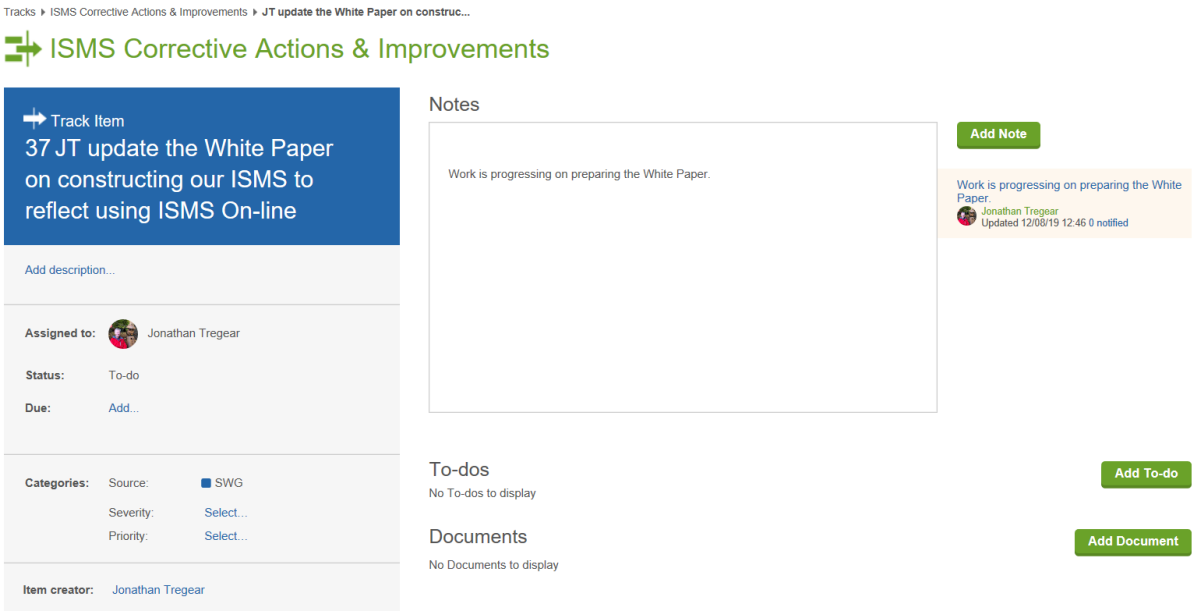


Figure 12 – Corrective Actions Details

Using this form, it is possible to:

- Assign the action to an individual,
- Assign a Due date for the action to be completed,
- Cross-reference the action to an ISO 27001 control,
- Jump to the relevant ISO 27001 control so that information about that control can be updated.

Once every 2 weeks the Security Working Party (SWP) reviews the open actions on this Actions list to ensure that they are being followed up.

Additional actions may be added to the list resulting from:

- Change Requests (See Section 3.7)
- Findings during Compliance Audits (See Section 3.8)
- Monitoring of Key Performance Indicators (See Section 3.10)
- Any report of a security incident or a weakness

3.7 Recording Change Requests

As a small company, we used to manage our change requests using a very simple Excel Spreadsheet to record what changes had been raised and the status of those change requests.

Once we started using ISMS On-line, we realised that we could use its Tracker system to provide a more professional approach for recording any changes that were raised and ensuring that they were properly authorised and followed up in accordance with our change management policies.

We created a Tracker to record all the changes that have been raised as shown below:

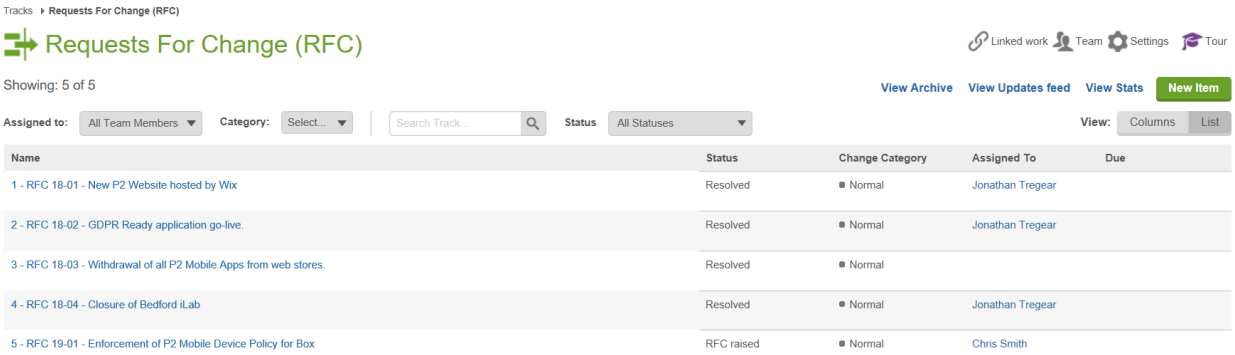


Figure 13 – List of Requests for Change

By selecting an individual change request, the details of the change can be viewed/edited as shown below:

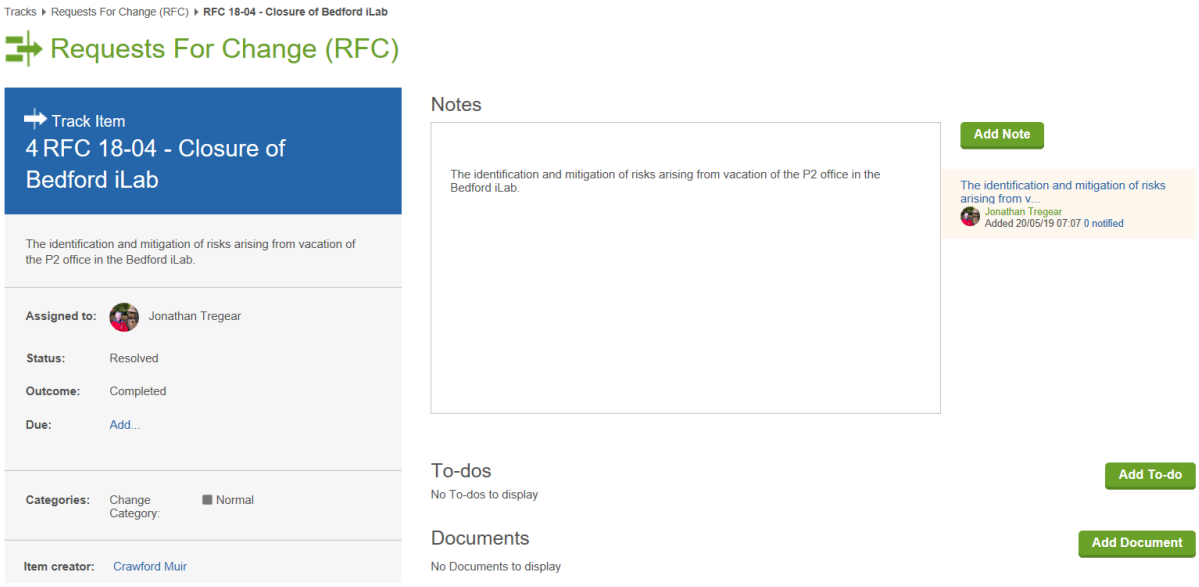


Figure 14 – Requests for Change Detail

This means that the change requests can be seen by the authorised people within the company, actions directly assigned to individuals to implement the change and the change can be linked to the ISO 27001 Statement of Applicability where appropriate.

3.8 Conducting Compliance Audits

To demonstrate that our policies were not simply ‘paperware’, we needed to put in place a Compliance Audit programme.

As part of our Compliance policy, we drew up an audit schedule which enabled us to set out a series of audits to ensure that we covered all the relevant ISO 27001 controls in a structured timescale. Each of the audits were allocated amongst the members of the SWP.

As shown below, ISMS On-line provides an in-built Project that allows you to record what audits you would like to conduct and when:

Figure 15 - Audit Programme

Most of our audits follow the conventional 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 setting out any non-conformities or observations and the audit report could be discussed at both the SWP and Security Working Group (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. We have even set up projects within ISMS to aid the distribution of these questionnaires to all members of staff for completion.

All non-conformities from any of these audits are recorded in the SWG Action list (See Section 3.6) and then monitored as part of the regular work of the SWP.

3.9 Using Policy Packs

ISMS On-Line provides several other functions which, whilst not pivotal, help improve the way in which security is run in an organisation.

One of these functions is called Policy Packs, which provides a way of grouping documentation together, distributing it to the relevant people and asking them to acknowledge their receipt and understanding of those policies.

The following image show a policy pack as it appears to the end user and how they can sign off that they have read, understood and undertake to comply with the pack

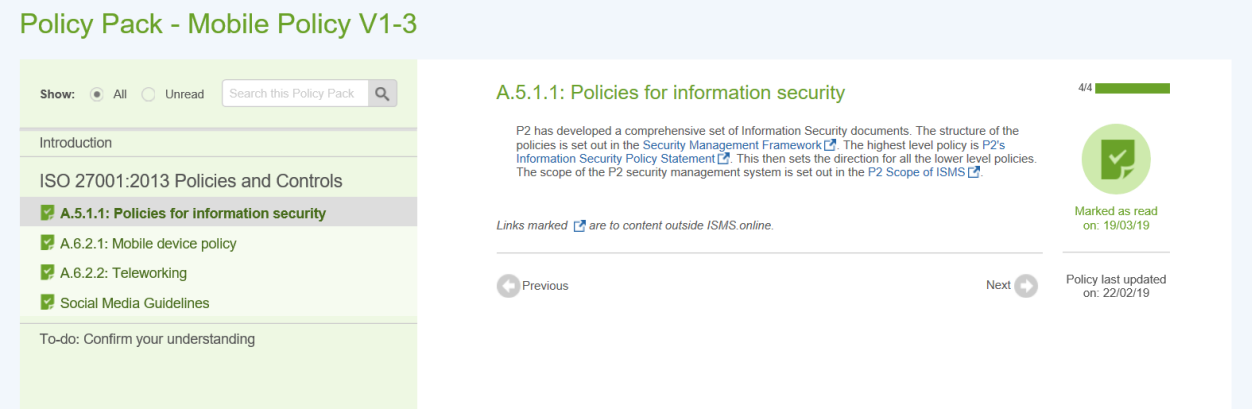


Figure 16 – Preparing and Completion of Policy Pack

As shown below, the person in charge of preparing the policy documents can then see how many people have read and marked as accepted those policies:

Figure 17 – Compliance with Policy Packs

Where necessary, the administrator can the specific people who have, or have not yet, signed up to the relevant policy pack as shown below:

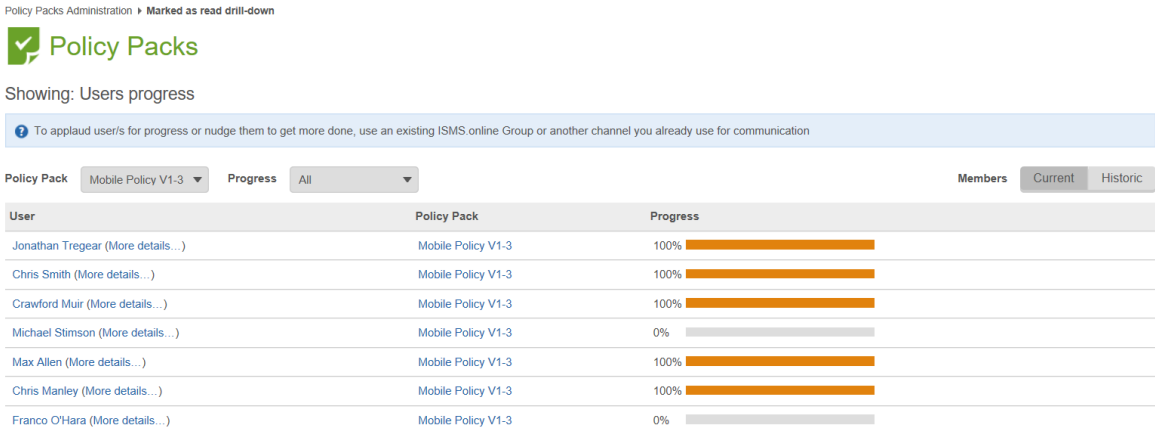


Figure 18 – Compliance with Policy Pack (Detail)

If you wish it is then straight-forward to use this information as a Key Performance Indicator which can also be monitored using features within ISMS On-line, as described in Section 3.10.

3.10 Defining and Monitoring Key Performance Indicators

Clause 9.1 of ISO 27001 states that there is a requirement for:

> Evaluation of the information security performance and effectiveness of the system. Includes what should be monitored, the measurement, analysis and evaluation, when and who does it, and who analyses and evaluates the results

In order to help meet this requirement, ISMS On-line contains a facility to define and monitor a series of Key Performance Indicators (KPI). Organisations can define as many KPIs as they want. ISMS On-Line Support for other Initiatives.

Amongst the KPIs that we have defined within our own ISMS are:

- Acknowledge of awareness and compliance with company policies
- Security score from Microsoft' Baseline Security Analyser
- Conducting service audits

3.11 Support for Business Continuity Planning

The flexibility built into ISMS On-line means that it is easy to see how it can be adapted to other management systems.

One particular area that is often closely related to information security is business continuity planning.

Building on our experience in the area of Business Continuity Planning, P2 has put together a series of projects and trackers that help organisations wishing to implement business continuity plans, especially those wishing for those plans to be certified against ISO 22301:2012 – Business Continuity Management Systems - Requirements.

We have grouped those projects and tracker into a Cluster as shown below:

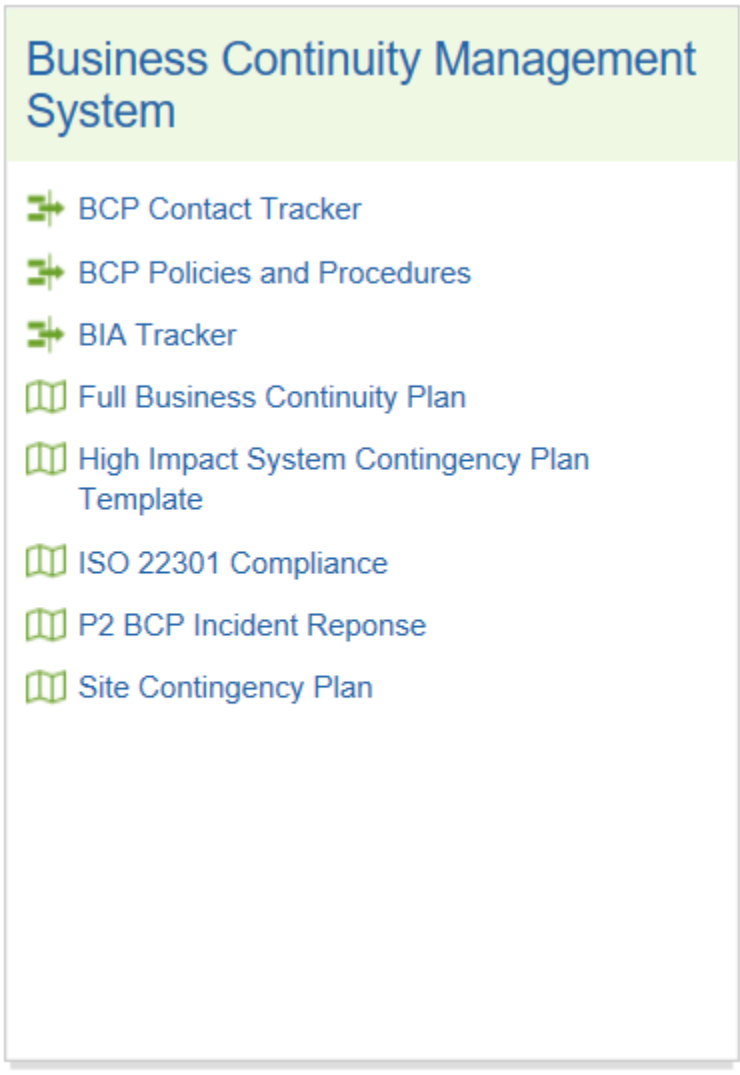
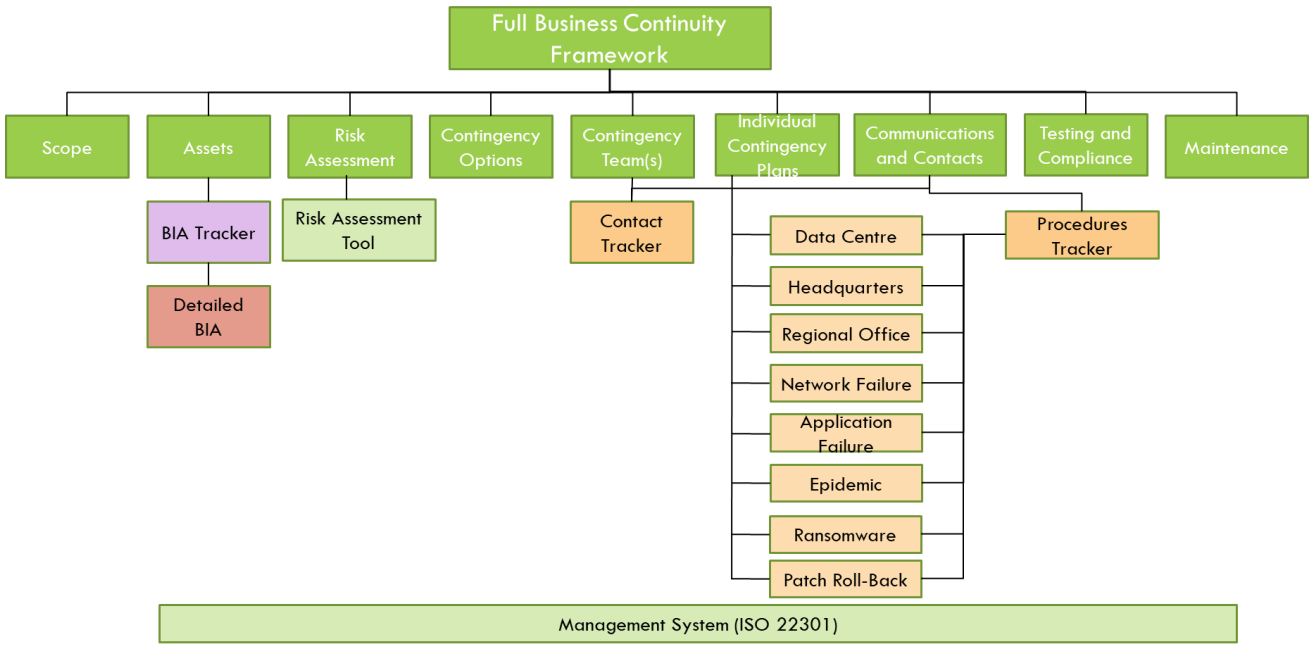


Figure 19 – List of Key Performance Indicators (KPIs)

The following figure shows the overall structure of these projects and plans and how they relate to each other



Please contact P2 at info@p2.co.uk if you want to further information on the support P2 can provide in this area.

3.12 Support for Quality Management Systems

There are strong parallels between maintaining the security of a system and ensuring that the organisation operates in accordance with well-defined quality procedures.

P2 is working with Alliantist on developing further projects and trackers to assist in demonstrating compliance against quality standards such as ISO 9001 and ensuring that those quality standards can be maintained.

4. CONCLUSIONS AND LESSONS LEARNT

Achieving ISO 27001 certification has improved our security policies and practices giving all of us a greater degree of confidence that we are handling our information in an appropriately secure manner. 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.

Using ISMS On-line has provided us with a flexible tool which helps us to have a common repository of information that significantly helps with communication and co-ordination, both of which are key to running our company in an efficient manner.

The flexibility that the software provides means that we can see opportunities for ISMS to help in a range of areas including business continuity, quality management and unified compliance management.

5. GLOSSARY

The following acronyms and abbreviations have been used in this report.

Acronym	Meaning
ISMS	Information Security Management System
KPI	Key Performance Indicators
P2	Platinum Squared
RPO	Recovery Point Objectives
RTO	Recovery Time Objective
SoA	Statement of Applicability
SWG	Security Working Group
SWP	Security Working Party

This Page Is Intentionally Blank