



JSC Consultants leverages web-based custom development solution to automate risk and action management and help organizations stay ISO 27001 compliant



Client Business Background

JSC Consultant Solutions Ltd is a consulting services company helping organizations with the design and implementation of management systems such as ISO 27001, ISO 9001, ISAE 3402, SOC1, SSAE 16, SOC2 & ISO 20000. They also do assessment work for the British Standards Institution, one of the leading certification bodies. They provide tools and automation software to other organizations which helps them increase their revenue, lower their cost, establish a platform for growth or prepare for M&A.

As a leading consultancy firm, its main aim is to provide a vast range of ISO certification services that help the client get certified to one of the coveted ISO standards. Our client was already having Office 365 license and using the platform for sharing documents with its clients who were not essentially SharePoint users.

Challenge

The client was already having a solution to manage risk and action using SharePoint. But it was not a centralized system. Every time the JSC consultants wanted to help their clients have access to the RMS, they had to share several documents, and create separate access for each account. The process was time taking and cumbersome.

- ◆ They wanted to create a comprehensive ISO 27001 Risk Management tool that could help their customers to manage any kind of risk, action, and documents without wasting time and effort.
- ◆ The customers could download the add-in from Microsoft AppSource and easily install on their environment. It could be a plug-in and play kind of RMS add-in.

- ◆ The tool should also help them implement ISO 27001 in their organization and help them stay compliant.
- ◆ They also wanted to have this tool run on Office 365 SharePoint environment, on either customer's Office 365 environment, or in case they don't have, JSC could let them access their environment.
- ◆ They also wanted to streamline the document sharing process for every customer.

Solution Strategy

We helped the client develop an online Microsoft SharePoint add-in for managing Information Security Management System (ISMS). The add-in could be easily downloaded from AppSource and hosted on their customer's environment or hosted on JSC's environment. The client's customers purchased the add-in within a subscription package, install in their environment and use instantly.

Along with major functionalities like email notifications, reminders, reporting dashboards, bulk data management (import/ export) and information search options, the add-in had four major modules:



The Risk Management Module :

The Risk Management module helps to determine risks based on assets, threats, and vulnerabilities. Users can add/ edit a new type of risk with their owners' detail. They can score the risks based on likelihood and impact and then select controls to mitigate any risks that are not accepted. The module helps to manage the risk treatment plan as well.



The Action Management Module

The Action Management module helps users to log a nonconformity, an incident, an event, an opportunity for improvement, or an action from the management review. Users determine root cause, corrective action, owners, plans, and deadlines from this module



The Recurring Action Management Module

The Recurring Action module helps users with all those recurring tasks that are built into any ISMS or QMS e.g. running an annual management review or a quarterly business continuity test exercise. In this module, users can set the action once. Action owners will get timely reminder emails to perform the action. It also enables users to record the outcome of the action (so one has evidence to show to the auditor) and once an action has been completed a new action will be set after the said frequency.



The Reporting Dashboard Module

There is an elaborate reporting dashboard that gives detailed insights on users' ISMS. Users can check detailed statistics on reports like:

- Overdue risks
- Root cause analysis
- Age of actions
- Overdue risk/actions by the owner
- Open/ close/ overdue risks and actions



Document Management simplified

As the add-in is built using the SharePoint platform, users get the advantage of its elaborate document management features which makes it easy to manage all the vast data and documents associated with the user's ISMS or QMS. Help Instructions and other important forms are also easily accessible within this comprehensive tool.



Email notifications and reminders

The various modules allow users to set due dates and review dates with automatic email reminders to action owners.



Bulk upload/ download of Risk and action data

The add-in allows users to upload excel files with complete risk or action data in a predefined format so bulk data can be uploaded into the system all at the same time. Similarly, bulk download of this data can also be managed using this tool.



Searching information

Another important thing which is faced by many organizations and its people is finding the right information easily. The add-in allows you to search easily with name/ detail related to any risk, action, or recurring action so users get the required information without scrolling through pages of data.



Results

Our client – JSC consultant got an automated SharePoint tool that could help several of its customers implement **ISO 27001 Risk Management System seamlessly into their systems.**

- ◆ The client got a centralized, add-in where Risks, actions, and documents all could be managed easily.
- ◆ They saved time, money, and efforts to manage and implement ISO certifications across their several customer accounts.
- ◆ The consultants saved efforts in installing the application on every customers' environment. Now JSC's customers- purchased the add-in from AppSource and start using instantly.
- ◆ The client could earn higher revenue and customer satisfaction through increased trust.
- ◆ Searching for the required information was easy than before.
- ◆ The client made better use of their Office 365 license thus making it a cost-effective solution

Screenshots

Action Number	Type	References	Date Raised	Date of Incident	Raised / Reported By	Owner	Issue	Cause Category	Cause(s)	Type of Incident	Containment Action	Corrective Action(s)	Review Date	Due Date
NCR0004	Information Security Incident	Reference from Team	02/06/2020 07:03	23/06/2020 07:03	sachin jain	sachin jain	Shared Drive not working for team members	Manpower		Incident			02/06/2020 07:03	07/06/2020 07:03
NCR0003	Information Security Incident	Missing Laptops	02/06/2020 01:32	01/06/2020 01:32	sachin jain	sachin jain	By monthly checkup found 5 Laptops are missing	Manpower		Incident			03/06/2020 01:33	01/06/2020 01:33
NCR0002	Opportunity for Improvement	Implementation of Cloud Computing	02/06/2020 12:31	03/06/2020 12:31	sachin jain	sachin jain	Cloud Computing budget increasing	Manpower					23/03/2020 12:32	27/04/2020 12:32
NCR0001	Nonconformity		02/06/2020 07:00	03/06/2020 07:00	sachin jain	sachin jain	Jun-1	Manpower		Incident			02/06/2020 07:00	28/04/2020 07:01
NCR0002	Opportunity for Improvement	Implementation of Cloud Computing	02/06/2020 12:31	03/06/2020 12:31	sachin jain	sachin jain	Cloud Computing budget increasing	Manpower					23/03/2020 12:32	27/04/2020 12:32
NCR0001	Nonconformity		02/06/2020 07:00	03/06/2020 07:00	sachin jain	sachin jain	Jun-1	Manpower		Incident			02/06/2020 07:00	28/04/2020 07:01
NCR0002	Opportunity for Improvement	Implementation of Cloud Computing	02/06/2020 12:31	03/06/2020 12:31	sachin jain	sachin jain	Cloud Computing budget increasing	Manpower					23/03/2020 12:32	27/04/2020 12:32

Action Management List

Add Action

* Fields are required.

Type

References

Date Raised *

Date of Incident *

Raised / Reported By (If O365 User)

Raised / Reported By Email (If External)

Owner (If O365 User)

Owner Email (If External)

Issue *

Cause Category

Cause(s)

Add New Action Form

Add Risk

* Fields are Required.

Asset Category *

Asset *

No. of Assets

Risk = Vulnerabilities and Threats *

Impact *

Date Raised *

Raised By (If O365 User)

Raised By Email (If External)

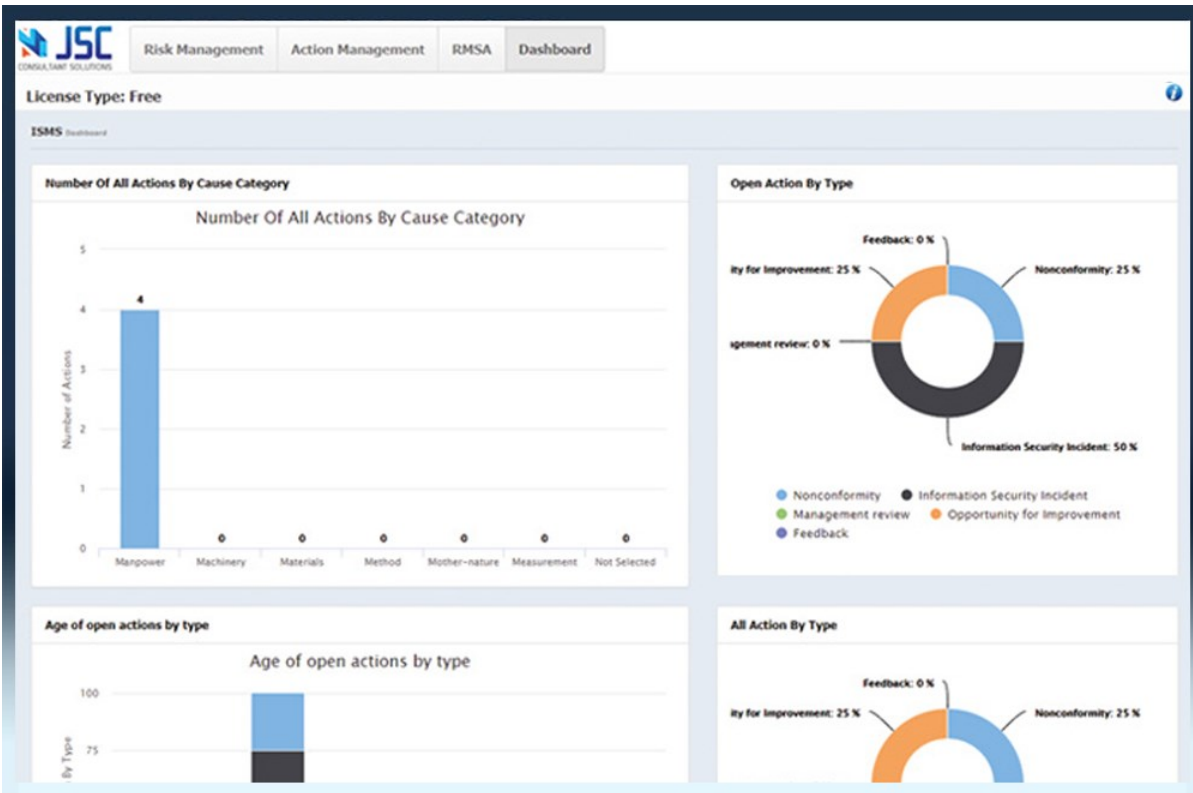
Likelihood

Impact

Risk

Risk Treatment Option

Add New Risk Form



Dashboard

Annual Action Management

Search:

RMSA Id	Task	Owner	Owner Email	Owner Email(NotO365)	Due Date	Frequency	Comment / Evidence	Reference	Reference Name	Action Closed	Close Date
<input type="checkbox"/> RMSA0001	Check that unauthorised privileges have not been obtained	Asset Owners	sachin.jain		01/06/2020 00:31	Biennial	Test	DOC 0	Information Security Classification	No	
<input type="checkbox"/> RMSA0002	Prepare report to the ISC	Asset Owners	sachin.jain		30/05/2020 00:33	Quarterly	Test	DOC 0	Responding to Information Security Reports	No	
<input type="checkbox"/> RMSA0005	Review if the maximum number of user licenses has been exceeded.	Systems Manager	sachin.jain		27/04/2020 04:13	Biennial		DOC 0	Information Security Continuity Planning	No	
<input type="checkbox"/> RMSA0002	Prepare report to the ISC	Asset Owners	sachin.jain		30/05/2020 00:33	Quarterly	Test	DOC 0	Responding to Information Security Reports	No	
<input type="checkbox"/> RMSA0005	Review if the maximum number of user licenses has been exceeded.	Systems Manager	sachin.jain		27/04/2020 04:13	Biennial		DOC 0	Information Security Continuity Planning	No	

Showing 1 to 3 of 3 entries

RMSA List

About ISO 27001 Risk Management add-in

This ISO 27001 Risk Management app will help anyone either implementing an ISO 27001 management system or anyone that has ISO 27001 implemented but are looking to have a tool that can help manage:

- The Information Security Management System
- Risks
- Nonconformities
- Corrective actions
- Information Security Incidents
- Opportunities for improvement
- Recurring tasks such as the quarterly restore test or the annual business continuity test

This ISO 27001 Risk Management app will send out email reminders when tasks are due for review or close to the deadline and the app will help tie the whole thing together in an online dashboard ready for your regular management review.

The ISO 27001 Risk Management app consist of the following modules:



The risk management module is based on an asset risk assessment process where you select assets, determine the risk, likelihood, impact, mitigation, treatment plan and residual risk. You would score the risks based on likelihood and impact and then select controls to mitigate any risks that are not accepted. The module will then help you manage the risk treatment plan as well.



The action module is where you log a nonconformity, an incident, an event, an opportunity for improvement or an action from your management review. You determine root cause, corrective action, owners, plans and deadlines.



The recurring action module is the module that will help you with all those recurring tasks that are built into your ISMS. These could for example be to run an annual management review or a quarterly business continuity test exercise. In this module you set the action once and the module will help remind you, it will enable you to record the outcome of the action (so you have evidence to show the auditor) and once an action has been done a new action will be set with the according to the chosen frequency.



Finally there is a dashboard that is reporting real time on your ISMS. It will for example report on

- Overdue risks
- Root cause analysis
- Age of actions
- Overdue risk/actions by owner

Information Page