How to conduct a Management Review Team Meeting

Conducting Management Review Team Meetings: a guide for Information Security Managers
Document Version Control

<table>
<thead>
<tr>
<th>Last Modified</th>
<th>Last Modified By</th>
<th>Document Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1 [DATE]</td>
<td></td>
<td>Document first created</td>
</tr>
</tbody>
</table>
Document Contents Page

Document Version Control ................................................................. 2

Document Contents Page ........................................................................ 3

ISO 27001 Clause 9.3 Management Review ........................................... 5

How to conduct a Management Review Meeting .................................... 6

Decide on Management Review Team attendees ................................... 6

Decide How Often to have a Management Review Meeting .................... 7

Book Your Meeting(s) ........................................................................ 7

Meeting Duration .............................................................................. 7

Prepare for the Management Review Meeting ....................................... 8

Create your agenda .......................................................................... 8

Send the Invite to the Management Review Team ................................. 9
Run The Meeting .................................................................................................... 9

Send out the minutes ............................................................................................ 10

Update Documents ............................................................................................... 10
ISO 27001 Clause 9.3 Management Review

Let us take a look at what the ISO 27001 requirement is for a management review before we step through the process of How to conduct a Management Review Team Meeting.

The ISO 27001 standard wants us to conduct regular, planned reviews of our information security management system to make sure that everything is working as it should. It is a fundamental part of the management system and as such it actually ticks a few of the ISO 27001 boxes. In particular it is address in ISO 27001 Clause 9.3 Management review and is one of the ISO 27001 mandatory documents.

The output and result of the meeting is a record of decisions made and changes needed. It is a requirement to keep copies of the meetings as evidence. It does have a structure agenda as per the Management Review Team Agenda Template. In brief it covers tracking of objectives, monitoring results, risk management, continual improvement, audit results and feedback.
How to conduct a Management Review Meeting

Decide on Management Review Team attendees

The Management Review Team attendees are documented in the roles and responsibilities document.

As a guide you ideally want as a minimum

- one representative from each in scope area
- one senior leadership representative

The management review team has oversight of the Information Security Management System, Risk Management and Continual Improvement. The exact responsibilities are documented in the Roles and Responsibilities document.

For now, decide on who will attend.
Decide How Often to have a Management Review Meeting

It is recommended that you have a management review meeting every month. This allows you to effectively manage, especially in the first year of an implementation. It is suggested that no less than every 3 months being at least 4 meetings a year.

Book Your Meeting(s)

It is good practice to set your meetings at the beginning of the year.

Be sure to book your meeting several weeks in advance to ensure availability.

Meetings can be conducted remotely over web collaboration tools such as Zoom, or Teams or meetings can be booked face to face in a meeting room.

If you book a meeting room, make sure that the room has a display screen that can be seen by all attendees.

Meeting Duration

Book a 1-hour meeting slot. On average a Management Review Meeting will take around 45 minutes. In time as you establish your information security management system and operating rhythm this time will reduce. If you over run additional meetings can be booked.
Prepare for the Management Review Meeting

Create a sub folder in your document storage for the meeting.

Collate the latest copies of the required documents for the Management Review Meeting and place them in the sub folder.

Ahead of the meeting, suggest 5 working days in advance, share links to the latest version of the documents with the invitees.

Note: confidential documents that should not be shared via email.

Consider your audience and the format they want to see the documents. You may require print outs, although this is discouraged. If required prepare them in advance.

Ensure that all of the documents are up to date and that all previous actions are updated.

Ensure people know if they are due to report back what is expected and in what format.

Create your agenda

Use the agenda template ‘Management Review Team Agenda – Template’
Complete the agenda and update the relevant sections.

**Send the Invite to the Management Review Team**

The Management Review Team are documented in the document Roles and Responsibilities. If not already sent, send the invite to the management review team and any guest attendees.

If the Management Review Team has changed update the document Roles and Responsibilities, remembering to update the version control.

**Run The Meeting**

The meeting requires a chairperson for the meeting. Decide on who will chair the meeting. The default is The Information Security Manager.

The meeting requires minuting. Decide on who will minute the meeting. The default is The Information Security Manager.

Work through the defined and structured agenda.

Agree / confirm the date of the next Management Review Meeting.
Send out the minutes

Within 5 working days send out links to the meeting minutes to all attendees.

Update Documents

Update appropriate management documentation based on the outcomes from the meeting. Documents to consider are

- Action Log
- Incident and Corrective Action Log
- Risk Register