

---

# DCSO Remediation Tracking Tool Operator's Handbook

Classification: Public  
Effective: 12.10.2017  
Version: 1.0

## Author

Incident Response Team  
+49 (30) 209664-0  
irt@dcso.de

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH  
Rosenthaler Str. 40  
10178 Berlin, Germany

## Content

<b>1. Introduction.....</b>	<b>2</b>
1.1 Communication Scheme.....	2
<b>2. Operators.....</b>	<b>3</b>
2.1 Prerequisites.....	3
2.2 Configure the Tool.....	3
2.3 Configure Outlook for Data-Import.....	4
2.4 Release a Package and Change a Status.....	4
2.5 Send Status-Request.....	5
2.6 Import Status Update and Issue Mails from Outlook.....	7
2.7 Modularized Dashboard.....	8
2.8 Reported Issues.....	9
2.9 Changelog.....	9
2.10 Deadlines.....	9
2.11 Reset Tracking Tool and Dashboard.....	10
2.12 Troubleshooting.....	10
<b>3. Project Members.....</b>	<b>12</b>
3.1 Prerequisites.....	12
3.2 Respond to Status Request Mail with new Status.....	12
3.3 Report Issue.....	13
<b>4. Modify Data Source .....</b>	<b>14</b>
4.1 Workpackages.....	14
4.2 Locations/Business Areas.....	15
4.3 States.....	16
4.4 Colors.....	16
4.5 Troubleshooting.....	17
<b>5. Sharing and Backup.....</b>	<b>17</b>
<b>6. Import New Tracking Tool Module.....</b>	<b>17</b>
<b>7. Recommendations.....</b>	<b>18</b>
<b>Appendix: Changelog .....</b>	<b>19</b>
DCSO Remediation Tracking Tool.....	19

# Operator's Handbook

## 1. Introduction

The DCSO Remediation Tracking Tool was developed during large scale security incidents to track remediation project/program milestones and progress. It enables quick information gathering and transparent global communication across different time zones during complex projects/programs, reducing the number of status calls significantly, whilst providing in-depth status overviews at the same time.

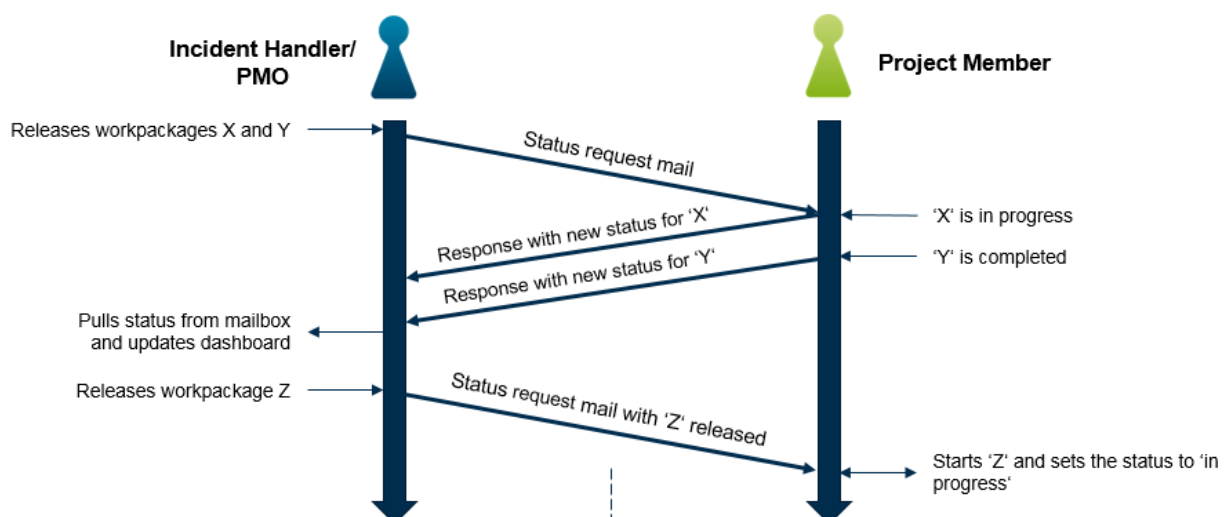
The Excel based tool integrates Outlook to create and send emails, containing the current status and links for the recipients to respond with a new status or an issue.

Using the customizable dashboard, it enables visualization of the progress in almost real-time, supporting managerial decisions and steering of remediation measures.

To operate the tool, Microsoft Office is required.

For out-of-band communication, a cloud hosted email-provider (e.g. Office365) can be used to avoid communication on compromised infrastructure.

### 1.1 Communication Scheme



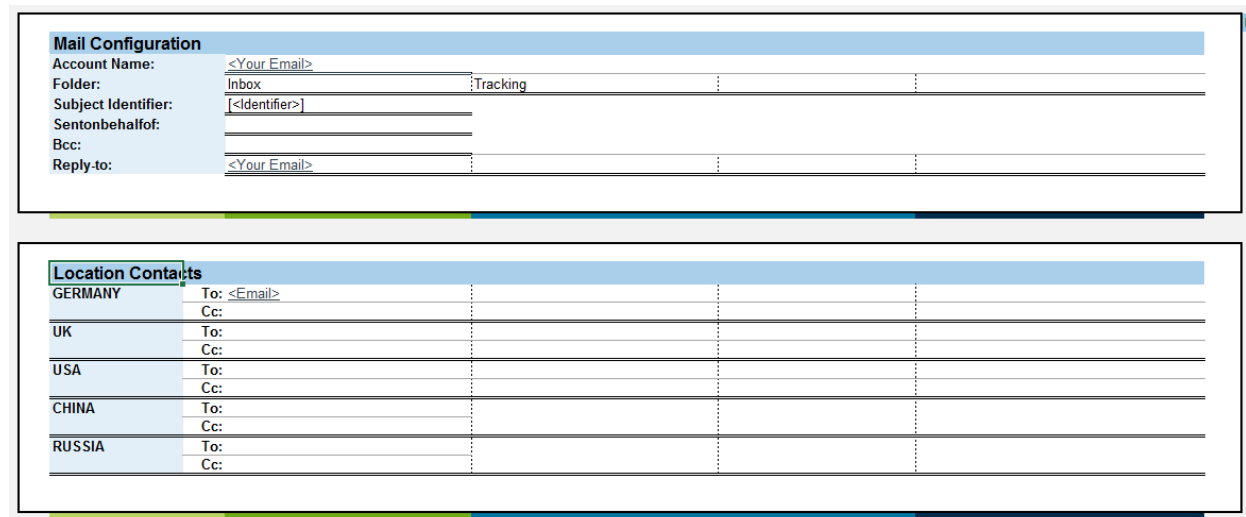
## 2. Operators

### 2.1 Prerequisites

- MS Office 2010 or later, including Office365 (VBA-Macro enabled Excel and Outlook)
- Central E-Mail address and hosting (e.g. Office 365, company)
  - For out-of-band communication and during remediation-event when there is no email communication possible, Office365 and Mailbox.org are recommended.

### 2.2 Configure the Tool

Go to the 'Configuration' sheet:



The screenshot shows two sheets from an Excel spreadsheet. The top sheet is titled 'Mail Configuration' and contains the following fields:

Account Name:	<Your Email>		
Folder:	Inbox	Tracking	
Subject Identifier:	<Identifier>		
Sentonbehalfof:			
Bcc:			
Reply-to:	<Your Email>		

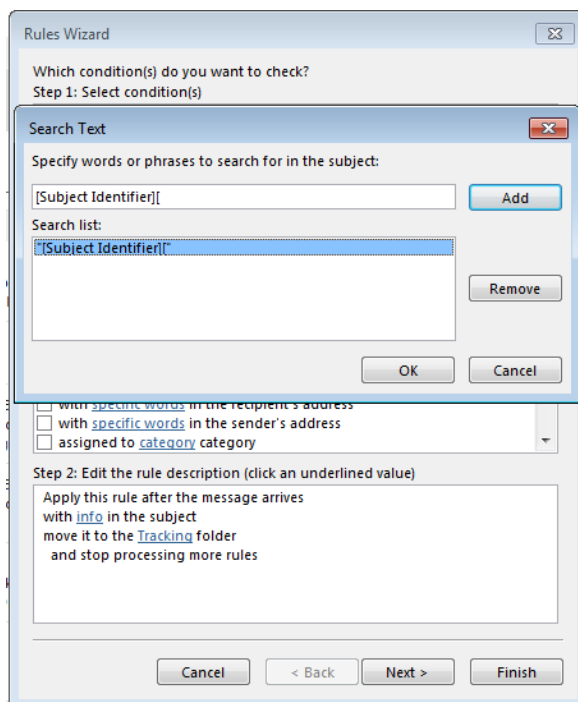
The bottom sheet is titled 'Location Contacts' and contains the following fields:

GERMANY	To: <Email>			
	Cc:			
UK	To:			
	Cc:			
USA	To:			
	Cc:			
CHINA	To:			
	Cc:			
RUSSIA	To:			
	Cc:			

- Required fields:
  - 'Account Name': Put in your E-Mail Account name (normally your E-Mail address).
  - 'Folder': Provide your email folder structure. To provide subfolders, use the next right field.
  - 'Subject Identifier': The identifier is required to identify status emails. Status E-Mail subjects will begin with this identifier.
  - 'Reply-To': Provide email addresses of persons who are supposed to track the project status. Status-response emails will be sent to the listed emails.
- Optional fields:
  - 'Sentonbehalfof': Provide another address to use as sender.
  - 'Bcc': Provide a BCC address. Status-request emails will be sent to the address.
- Location contacts:
  - Provide addresses of the contacts who should receive status requests.
  - To provide more than one address, fill in the fields to the right.

## 2.3 Configure Outlook for Data-Import

- Create an E-Mail folder in which all status update and issue report mails will be moved.
  - E.g.: Inbox/Tracking
- Create a rule to move all status-response and issue report mails to the folder.
- The rule should check for '[**Subject Identifier**][' in the subject. The last open bracket '[' is important, as it differentiates response mails from request mails.



- The rule should not move **request** mails to the tracking folder, to prevent parsing errors during import.

## 2.4 Release a Package and Change a Status

It is possible to release and change status of each package for each location or globally.

Go to the 'Start packages' sheet.

CHANGE STATUS				
Change status for package		to status		
PM-BLKI Block Internet Connection		released	Change for all Sites	
1		2		
Change status in site		for package	to status	
BRAZIL	PM-CMPS Identify Compromised Systems	released	Change in Site	
3	4	5		

To release or change a status of a package

- globally:
  - Choose the package from the dropdown list in field 1.
  - Choose the status in field 2.
  - Click on 'Change for all Locations'.
- for a specific location:
  - Select the location and package in field 3 and 4.
  - Choose the status in field 5.
  - Click on 'Change in Location'.

A status request should be sent to the corresponding sites after releasing a package (2.5).

## 2.5 Send Status-Request

Go to the 'Start packages' sheet.

Choose the location in the dropdown list and click on 'Send status Email'.

15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			

<b>SEND STATUS</b>	
<input type="button" value="Send status Email"/>	
	To
Site	SWEDEN

An Outlook window will pop up:

Send To... **IT Forensics & Incident Response (IRT):**

Cc...

Subject [Subject Identifier] Status from 7/25/2017 at 12:02:31 PM for UK

Dear colleagues,

Please find below the status for the location **UK** as of **7/25/2017 at 12:02:31 PM**.

Please update the information using the status links provided in the table below.

Work Packages for the Location UK	Status	Time	Report Issue	New Status
<a href="#">PM-CMPS Identify Compromised Systems</a>	completed	7/24/2017 5:06:09 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>
PM-REBS Rebuild Servers	in progress	7/18/2017 4:32:47 PM	<a href="#">Issue</a>	<a href="#">completed evidence provided</a>
PM-REBC Rebuild Clients	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-PWCC Password Change for Privileged Local Accounts	completed	7/24/2017 5:06:17 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>
PM-KTGT Kerberos TGT Reset	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLKI Block Internet Connection	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLKS Block System-To-System Connection	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLIP IP Blacklisting	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-SHDN Sinkhole Domain Names	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-PWCE Enterprise Password Change	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-WHIT Application Whitelisting on DCs	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-MVUL Scan for vulnerable Middleware components	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-MHRD Middleware hardening	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-AWRN: Awareness	completed	7/18/2017 4:30:27 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>

Many thanks in advance

Verify that the email address is correct and click on 'Send' to send the mail.

- To modify the content of the request, response and issue mails, click on the plus sign on the left side to reveal the html code. Do not modify capitalized strings, as they will be modified by the VBA macro.

SEND STATUS	
Send status Email	
To	
Location	UK
Subject	SUBJECTID Status from CURRENTDATE for Location
Head	<p>&lt;p&gt;Dear colleagues,&lt;br&gt;</p> <p>&lt;p&gt;Please find below the status for the businessarea</p> <p>&lt;strong&gt;BUSINESSAREA&lt;/strong&gt; as of &lt;strong&gt;CURRENTDATE&lt;/strong&gt;.</p> <p>Please update the information using the status links provided in the table below.&lt;br&gt;&lt;/p&gt;</p> <p>&lt;br&gt;</p> <p>&lt;table style="border: solid 1px" cellspacing=0 cellpadding=5&gt;</p>

## 2.6 Import Status Update and Issue Mails from Outlook

Go to the 'OutlookImport' sheet and click on 'Import from Outlook'.

From	Subject	Date	Code						
ZZZ	[Subject Identifier][020103] Status changed	7/18/2017 16:30	020103						
YYY	[Subject Identifier][021604] Status changed	7/18/2017 16:30	021604						
XXX	[Subject Identifier][020203] Status changed	7/18/2017 16:32	020203						

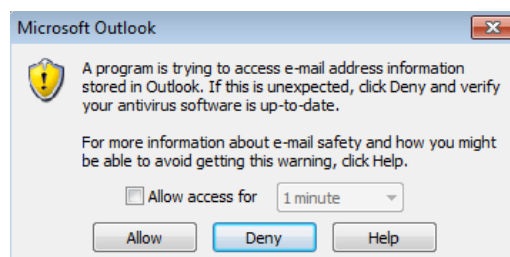
Import from Outlook

Re-apply IDs

Automatic Import ON

Automatic Import OFF

- If a warning window pops up, click on 'Allow'.



New imports will be added to the list and the dashboard will be updated automatically.

Reapply changes by clicking 'Re-apply IDs'.

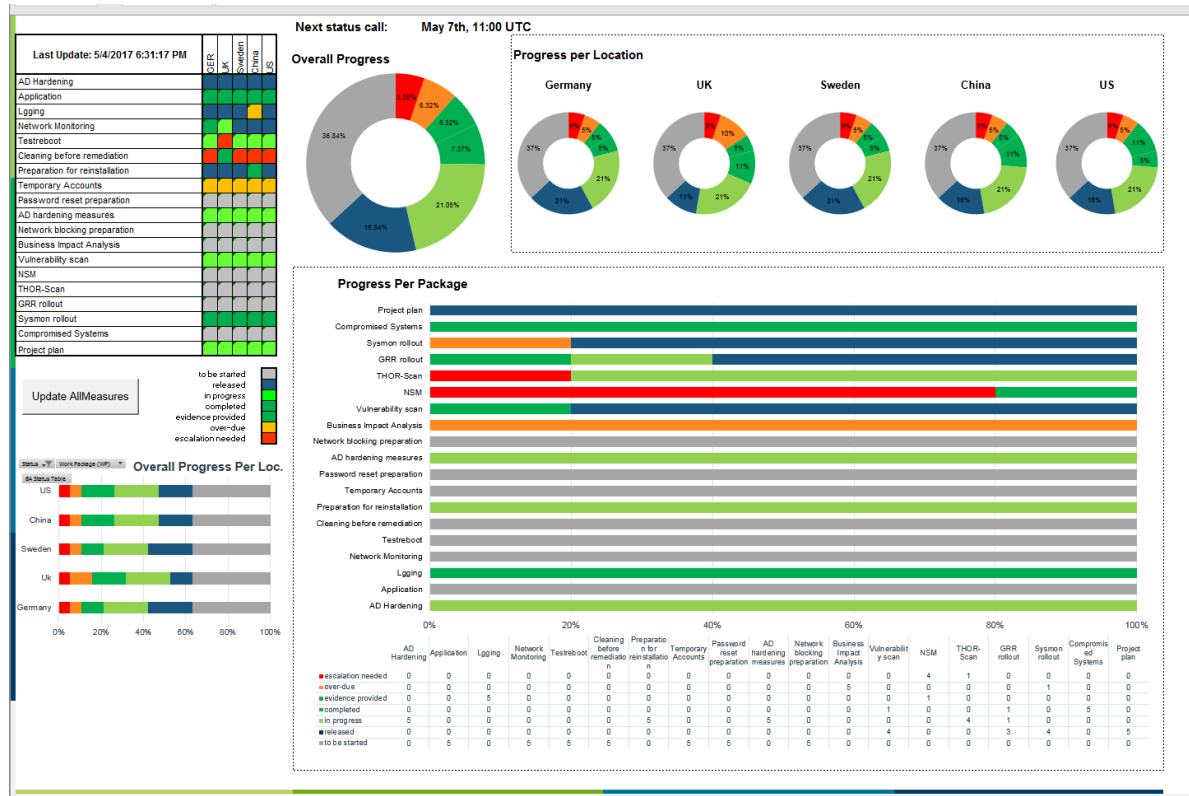
To automatically import new status every minute, click on 'Automatic Import ON'.

To deactivate automatic import, click on 'Automatic Import OFF'.



## 2.7 Modularized Dashboard

The Remediation Tracking Tool comes with a standard dashboard in the sheet 'Dashboard'.



- It is possible to rearrange and modify all modules of the dashboard besides the status matrix, which is generated by VBA code.
- Dashboard modules can be found in the sheet 'DashboardModules' and used to create new dashboards.
- Issues are shown below the Dashboard:

			to be started						
			3	3	3	3	3	3	3
<b>ISSUES</b>									
PM-MHRD Middleware hardening	Solved	USA has Issues with the Work Package "PM-MHRD" Please							
PM-BLKI Block Internet Connection	Unsolved	USA has Issues with the Work Package "PM-BLKI" Please							
PM-BLKI Block Internet Connection	Solved	UK has Issues with the Work Package "PM-BLKI" Please							
PM-REBS Rebuild Servers	Unsolved	GERMANY has Issues with the Work Package "PM-REBS"							
PM-CMPS Identify Compromised Sys	Unsolved	Issue							

## 2.8 Reported Issues

The 'Issues' sheet shows reported issues.

Change the status to solved using the dropdown menu.

Number of read i	5						
Last read Issue:	7/18/2017 16:55						
Location	Work Package	Reported By	Subject	Issue	Date	Code	Status
USA	PM-MHRD Middleware hardening	XXX	[Subject Identifier][031500][ISSUE] Status changed	USA has Issues with the Work Package "PM-MHRD" Please describe your Issue:	7/18/2017 16:55	31500	Solved
USA	PM-BLKI Block Internet Connection	XXX	[Subject Identifier][030600][ISSUE] Status changed	USA has Issues with the Work Package "PM-BLKI" Please describe your Issue:	7/18/2017 16:41	30600	Unsolved
UK	PM-BLKI Block Internet Connection	XXX	[Subject Identifier][020600][ISSUE] Status changed	UK has Issues with the Work Package "PM-BLKI" Please describe your Issue:	7/18/2017 10:26	20600	Solved
GERMANY	PM-REBS Rebuild Servers	XXX	[Subject Identifier][010200][ISSUE] Status changed	GERMANY has Issues with the Work Package "PM-REBS" Please describe your Issue:	7/18/2017 10:25	10200	Unsolved
GERMANY	PM-CMPS Identify Compromised Systems	XXX	[Subject Identifier][010105][ISSUE] Status changed	Issue	7/17/2017 15:58	10105	Unsolved

## 2.9 Changelog

The changelog provides a history of all the status changes:

	A	B	C	D	E	F
1	Workpackage	Status	Location	Date	Reported/Manual	
2	PM-CMPS Identify Compromised Systems	in progress	UK	7/18/2017 16:30	Reported	
3	PM-AWRN: Awareness	completed	UK	7/18/2017 16:30	Reported	
4	PM-REBS Rebuild Servers	in progress	UK	7/18/2017 16:32	Reported	
5	PM-CMPS Identify Compromised Systems	completed	All locations	7/24/2017 17:06	Manual	
6	PM-PWCC Password Change for Privileged Lo	completed	All locations	7/24/2017 17:06	Manual	
7						

The changelog is not deleted, when only tracking is reset.

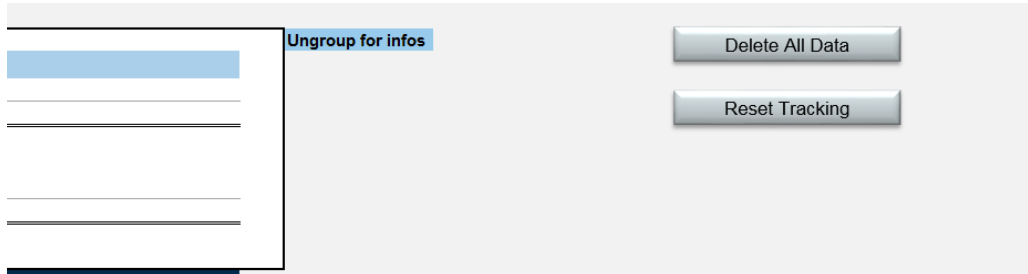
## 2.10 Deadlines

Deadlines can be provided in the 'Deadlines' table:

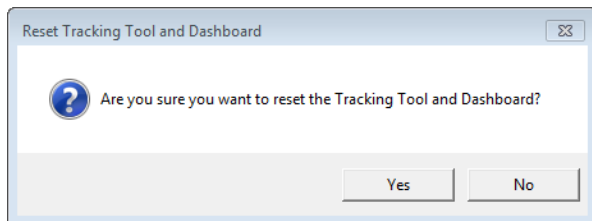
Is calculated automatically			
Work Package	Deadline	Over-due	Issue
PM-CMPS Identify Compromised Systems	4/1/17 12:00 AM	TRUE	
PM-REBS Rebuild Servers	4/4/18 6:00 PM	FALSE	
PM-REBC Rebuild Clients	4/25/17 6:00 PM	TRUE	
PM-PWCC Password Change for Privileged Lo	4/26/17 6:00 PM	TRUE	
PM-KTGT Kerberos TGT Reset	4/27/17 6:00 PM	TRUE	
PM-BLKI Block Internet Connection	4/28/17 6:00 PM	TRUE	
PM-BLKS Block System-To-System Co	4/29/17 6:00 PM	TRUE	
PM-BLIP IP Blacklisting	4/30/17 6:00 PM	TRUE	
PM-RMAC Replace RAT	5/1/17 6:00 PM	TRUE	
PM-SHDN Sinkhole Domain Names	5/2/17 6:00 PM	TRUE	
PM-PWCE Enterprise Password Chang	5/3/17 6:00 PM	TRUE	
PM-ESAE Implement ESAE	5/4/17 6:00 PM	TRUE	
PM-WHIT Application Whitelisting on D	5/5/17 6:00 PM	TRUE	
PM-MVUL Scan for vulnerable Middlew	5/6/17 6:00 PM	TRUE	
PM-MHRD Middleware hardening	5/7/17 6:00 PM	TRUE	
PM-AWRN: Awareness	5/8/17 6:00 PM	TRUE	

## 2.11 Reset Tracking Tool and Dashboard

To only reset the tracking and dashboard, go to the 'Configuration' sheet:



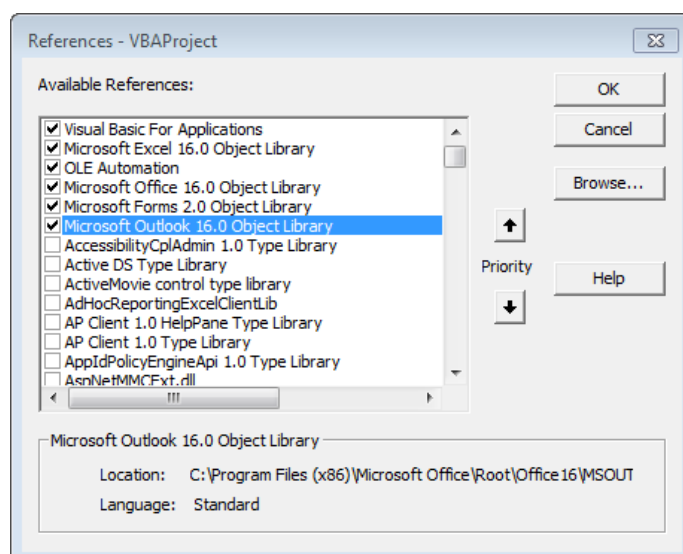
Click on 'Reset Tracking' and confirm reset.



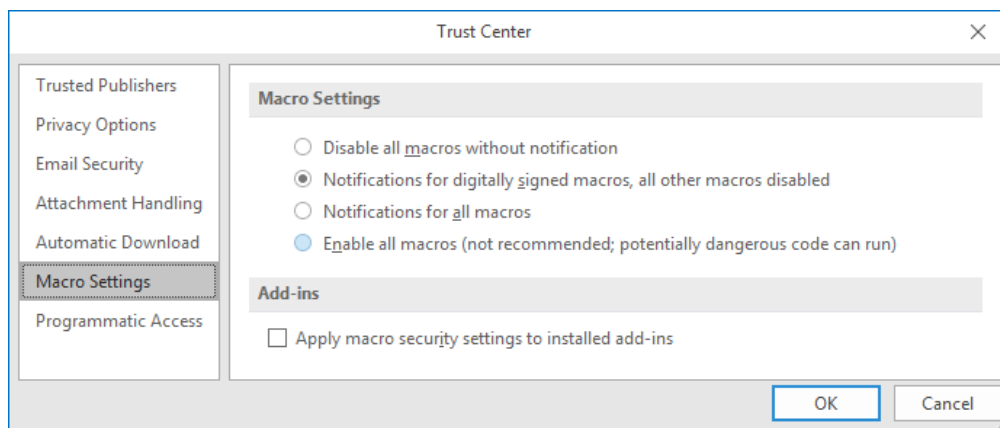
To reset all sheets, click on 'Delete All Data'.

## 2.12 Troubleshooting

- VBA compilation error
  - Make sure that VBA macros are enabled.
- VBA compilation error due to missing MS Office Object Library
  - In the Visual Basic Editor (ALT+F11), select References from the Tools menu:



- Scroll down the list of available references until you encounter the required object library according to your Office version (e.g. MS Outlook 14.0 Object Library).
- Find the required libraries in the screenshot above.
- Error during import / import fails:
  - Make sure you correctly put in your account name and tracking folders in 'Configuration' sheet. The account name can be found on the top of the email folders view in Outlook.
  - Check security settings in Outlook.
- VBA macros cannot be executed at all:
  - Make sure your Office settings allow the execution of VBA macros.
  - Find the settings in 'Options' > 'Trust Center' > 'Trust Center Settings...'



### 3. Project Members

Project members do not have to make any configurations. Providing a status update is as simple as clicking on a link provided by email.

This can also be done using a smart phone.

#### 3.1 Prerequisites

- HTML capable E-Mail reader (e.g. each smart phone, Outlook, Webmail, etc.)

#### 3.2 Respond to Status Request Mail with new Status

Users will receive a status request email similar to the following:

Dear colleagues,

Please find below the status for the location **UK** as of **7/25/2017 at 12:02:31 PM**.

Please update the information using the status links provided in the table below.

Work Packages for the Location UK	Status	Time	Report Issue	New Status
<a href="#">PM-CMPS Identify Compromised Systems</a>	completed	7/24/2017 5:06:09 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>
PM-REBS Rebuild Servers	in progress	7/18/2017 4:32:47 PM	<a href="#">Issue</a>	<a href="#">completed evidence provided</a>
PM-REBC Rebuild Clients	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-PWCC Password Change for Privileged Local Accounts	completed	7/24/2017 5:06:17 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>
PM-KTGT Kerberos TGT Reset	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLKI Block Internet Connection	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLKS Block System-To-System Connection	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-BLIP IP Blacklisting	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-SHDN Sinkhole Domain Names	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-PWCE Enterprise Password Change	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-WHIT Application Whitelisting on DCs	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-MVUL Scan for vulnerable Middleware components	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-MHRD Middleware hardening	to be started	7/24/2017 5:16:10 PM	<a href="#">Issue</a>	None
PM-AWRN: Awareness	completed	7/18/2017 4:30:27 PM	<a href="#">Issue</a>	<a href="#">evidence provided</a>

Many thanks in advance

Select the status for the released packages by clicking on the provided links in the column 'New Status'.

For each status update a new message window will open:

[Subject Identifier][020603] Status changed - Message (HTML)

To...

Cc...

Send

Subject

The businessarea BRAZIL has changed the status of the Work Package "PM-BLKI Block Internet Connection" to "in progress".

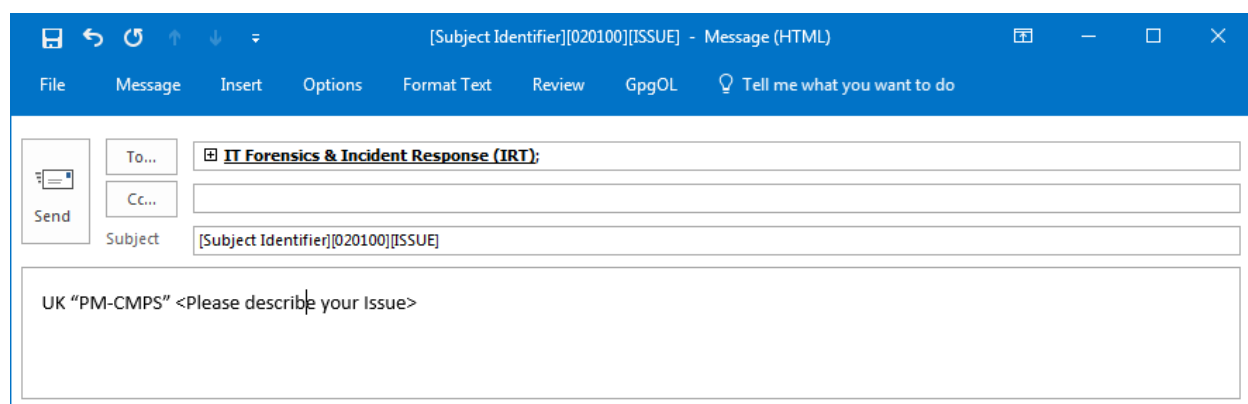
Click on 'Send' to send the response mail.

- The subject must not be modified.
- In case a false status was reported, contact the project manager to provide the correct status, so he can update his data.

### 3.3 Report Issue

To report an issue, click on 'Issue' in the 'Report Issue' column.

A new message window will pop up:



[Subject Identifier][020100][ISSUE] - Message (HTML)

File Message Insert Options Format Text Review GpgOL Tell me what you want to do

Send

To... IT Forensics & Incident Response (IRT);

CC...

Subject [Subject Identifier][020100][ISSUE]

UK "PM-CMPS" <Please describe your Issue>

Describe your issue in the mail body and click on 'Send'.

## 4. Modify Data Source

This part of the manual describes how an operator can add or remove locations, workpackages and status. Adding or modifying data requires a reset of the Tracking Tool.

Keep in mind that modifying the data source probably breaks the pivot tables and render the dashboard useless. In that case, modify the pivot tables in the sheet 'Pivot Tables' and create a new dashboard.

### 4.1 Workpackages

Go to the sheet 'IDs' and find the workpackages state table:

	A	B	C	D	E	F	G	H	I
1	Workpackages	ID	State1	State2	State3	State4	State5	WP Short ID	URL
2	PM-CMPS Identify Compromised Systems	01	to be started	released	in progress	completed	evidence provided	PM-CMPS	
3	PM-REBS Rebuild Servers	02	to be started	released	in progress	completed	evidence provided	PM-REBS	
4	PM-REBC Rebuild Clients	03	to be started	released	in progress	completed	evidence provided	PM-REBC	
5	PM-PWCC Password Change for Privileged Local Account	04	to be started	released	in progress	completed	evidence provided	PM-PWCC	
6	PM-KTGT Kerberos TGT Reset	05	to be started	released	in progress	completed	evidence provided	PM-KTGT	
7	PM-BLKI Block Internet Connection	06	to be started	released	in progress	completed	evidence provided	PM-BLKI	
8	PM-BLKS Block System-To-System Connection	07	to be started	released	in progress	completed	evidence provided	PM-BLKS	
9	PM-BLIP IP Blacklisting	08	to be started	released	in progress	completed	evidence provided	PM-BLIP	
10	PM-RMAC Replace RAT	09	to be started	released	in progress	completed	evidence provided	PM-RMAC	
11	PM-SHDN Sinkhole Domain Names	10	to be started	released	in progress	completed	evidence provided	PM-SHDN	
12	PM-PWCE Enterprise Password Change	11	to be started	released	in progress	completed	evidence provided	PM-PWCE	
13	PM-ESAE Implement ESAE	12	to be started	released	in progress	completed	evidence provided	PM-ESAE	
14	PM-WHIT Application Whitelisting on DCs	13	to be started	released	in progress	completed	evidence provided	PM-WHIT	
15	PM-MVUL Scan for vulnerable Middleware components	14	to be started	released	in progress	completed	evidence provided	PM-MVUL	
16	PM-MHRD Middleware hardening	15	to be started	released	in progress	completed	evidence provided	PM-MHRD	
17	PM-AWRN: Awareness	16	to be started	released	in progress	completed	evidence provided	PM-AWRN	
18									
19									

- Remove a workpackage:
  - To remove a package, delete the corresponding row by right clicking on the row and choosing 'Delete' and 'Table Rows'
  - Correct the ID numbers in the ID column to an ongoing number.
  - Click on 'Update Data' button to regenerate the dashboard matrix and deadline sheet.
- Add a workpackage:
  - To add a package, right click on the last row of the table and insert a table row by clicking on 'Insert' and 'Table Row Below'.
  - Put in the package name, number and states.
  - 'WP Short ID' and 'URL' are optional.

13	PM-ESAE Implement ESAE	12	to be started	released	in progress	completed	evidence provided	PM-ESAE	
14	PM-WHIT Application Whitelisting on DCs	13	to be started	released	in progress	completed	evidence provided	PM-WHIT	
15	PM-MVUL Scan for vulnerable Middleware components	14	to be started	released	in progress	completed	evidence provided	PM-MVUL	
16	PM-MHRD Middleware hardening	15	to be started	released	in progress	completed	evidence provided	PM-MHRD	
17	PM-AWRN: Awareness	16	to be started	released	in progress	completed	evidence provided	PM-AWRN	
18	New Package	17	to be started	released	in progress	completed	evidence provided	Optional	
19									

- Reset the Tracking Tool, by clicking on 'Reset Tracking' button.
- Click on 'Update Data' button to regenerate the dashboard matrix and deadline sheet.

## 4.2 Locations/Business Areas

Go to the sheet 'IDs':

Business Area	ID	In scope	Group
GERMANY	01	Yes	1
UK	02	Yes	1
USA	03	Yes	1

- Remove a location:
  - To remove a location, delete the corresponding row by right clicking on the row and choosing 'Delete' and 'Table Row'
  - Go to the dashboard in 'Dashboard'.
  - Remove the corresponding Column from the matrix, by right clicking on that column and selecting 'Delete' and 'Table Column'.
  - Click on 'Update Data' button to regenerate the dashboard matrix and deadline sheet.
- Add a location:
  - To add a location, right click on the last row of the table and insert a table row by clicking on 'Insert' and 'Table Row Below'.
  - Put in the location name, ID number and the other fields.
  - Click on 'Update Data' button to regenerate the dashboard matrix and deadline sheet.
- Reset the Tracking and Dashboard, by clicking on 'Reset Tracking' in sheet 'IDs'.
- Reset Tracking, Dashboard and all other sheets, by clicking on 'Delete All Data'.
- Go to the 'Configuration' sheet and add the location and the email addresses of the project members to the contacts section:

Business Area Contacts				
Germany	To:	dcso.de		
	Cc:			
UK	To:			
	Cc:			
Sweden	To:			
	Cc:			
China	To:			
	Cc:			
US	To:			
	Cc:			



## 4.3 States

Go to the sheet 'IDs' and find the state table:

State	ID	Color	To Be Set	See action
to be started	01	LightGrey	Central	No
released	02	Blue	Company	Yes
in progress	03	LightGreen	Company	Yes
completed	04	Green	Company	Yes
evidence provided	05	Green	Company	Yes

- Add or remove a row to add or remove a state.
  - Assign a color from the dropdown list.
  - Choose if a status can only be updated by the admin ('Central').
  - 'See action' sets the state to hidden.
- Add or remove state columns in the workpackages states table accordingly:

	A	B	C	D	E	F	G	H
1	Workpackages	ID	State1	State2	State3	State4	State5	WP Short ID
2	PM-CMPS Identify Compromised Systems	01	to be started	released	in progress	completed	evidence provided	PM-CMPS
3	PM-REBS Rebuild Servers	02	to be started	released	in progress	completed	evidence provided	PM-REBS
4	PM-REBC Rebuild Clients	03	to be started	released	in progress	completed	evidence provided	PM-REBC
5	PM-PWCC Password Change for Privileged Local Account	04	to be started	released	in progress	completed	evidence provided	PM-PWCC
6	PM-KTGT Kerberos TGT Reset	05	to be started	released	in progress	completed	evidence provided	PM-KTGT
7	PM-BLKI Block Internet Connection	06	to be started	released	in progress	completed	evidence provided	PM-BLKI
8	PM-BLKS Block System-To-System Connection	07	to be started	released	in progress	completed	evidence provided	PM-BLKS
9	PM-BLIP IP Blacklisting	08	to be started	released	in progress	completed	evidence provided	PM-BLIP
10	PM-BLIP IP Blacklisting	09	to be started	released	in progress	completed	evidence provided	PM-BLIP

## 4.4 Colors

Go to the sheet 'IDs' and find the color table:

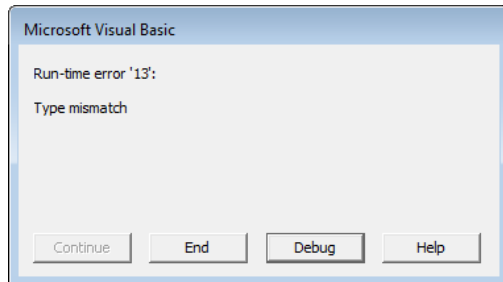
Color	R	G	B
Red	255	51	0
Green	113	171	26
Grey	128	128	128
Amber	255	192	0
White	255	255	255
LightGrey	192	192	192
LightGreen	184	210	100
Blue	0	116	161

Put in the RGB code of your desired color.

## 4.5 Troubleshooting

If you have any questions please don't hesitate to contact DCSO and we are happy to help you.

- Run-time error: Type mismatch



There is a chance that the updating the dashboard fails because of a type mismatch error.

In most cases, this is related to the status matrix.

Make sure that names of packages and locations are set correctly and check the formulas. Formulas should be referencing the according row and column.

- The dashboard and its modules are broken:

That is because pivot tables used to generate dashboard modules have changed. Pivot tables use the generated 'Tracking' sheet as their data source. Modifying the data source, and thus the tracking sheet, can break pivot tables.

Find the pivot tables in the sheet 'Pivot Tables'. Try to modify the pivot tables, so that they look like the standard functioning ones.

## 5. Sharing and Backup

For sharing or backup, simply send or backup the Excel file, as all data is saved in the file.

## 6. Import New Tracking Tool Module

To update the tool, put the 'TrackingTool.bas' file into the same directory as the Tracking Tool Excel file.

Then, go to the 'Configuration' sheet and click on the button 'Import New Tracking Tool Module' on the right. This will replace your current module.

## 7. Recommendations

- Status Synchronization between project team members:  
Overall status should be synchronized regularly, to avoid misstates. This can be done through regular distribution of the Tracking Tool itself. A way to do this is by having a regularly updated version of the tool on a share, where it is accessible by all project members for synchronization.
- Outlook rule should never move request mails to the tracking folder, as these will cause an error during import.
- Using a cloud hosted email-provider (e.g. Office365) the tool can be used for out-of-band communication to avoid communication on compromised infrastructure.

## Appendix: Changelog

### DCSO Remediation Tracking Tool

Ver.	Date	Change	Developer
0.1	29.03.17	Initial release	Dr. Andreas Rohr Daniel Nguyen
0.2	23.06.17	<ul style="list-style-type: none"> <li>- Created new pivot tables and dashboard elements</li> <li>- Changed the code and data model to add or remove data without changing the VBA code</li> <li>- Added 'Dashboard Modules' sheet</li> <li>- Added 'Deadlines' sheet</li> <li>- Rearranged code for simpler reading</li> </ul>	Daniel Nguyen
0.3	25.07.17	<ul style="list-style-type: none"> <li>- Added Issue Reporting Functionality</li> <li>- Added Automatic Import</li> <li>- Added Changelog</li> <li>- Rearranged code for simple import/export of VBA code</li> <li>- Added Reset All Data Button to 'Configuration' sheet</li> <li>- Changed Sheet 'AllMeasures' to 'Dashboard'</li> <li>- Added Issue table to dashboard</li> <li>- Added timestamps to 'Tracking' sheet</li> <li>- Rearranged sheets</li> </ul>	Daniel Nguyen
0.4	09.08.17	<ul style="list-style-type: none"> <li>- 'Delete All Data' button updated and now asks for verification before resetting each sheet</li> <li>- Added functionality to regenerate dashboard matrix and deadline table</li> </ul>	Daniel Nguyen
1.0	10.10.17	<ul style="list-style-type: none"> <li>- Added 'Import New Tracking Tool Module' button</li> </ul>	Daniel Nguyen