

---

# DCSO Remediation Tracking Tool Project Member'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

# Project Member'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.

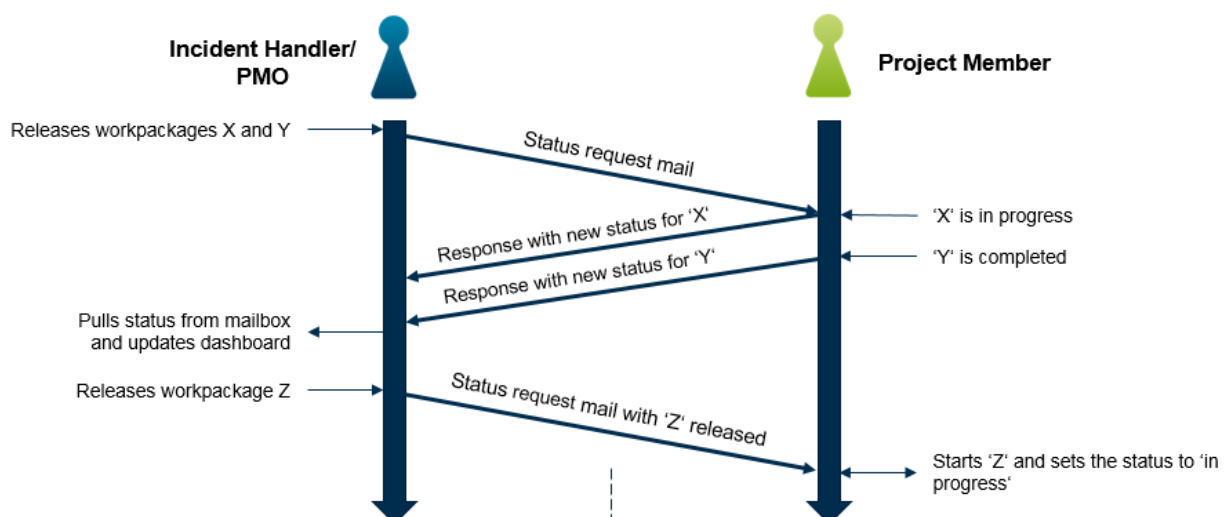
The Excel based tool integrates Outlook to create and send emails, containing the current status and links for the recipients to respond with a new status or an issue.

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



An Outlook window will pop up:

## 2. 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.

### 2.1 Prerequisites

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

### 2.2 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**.

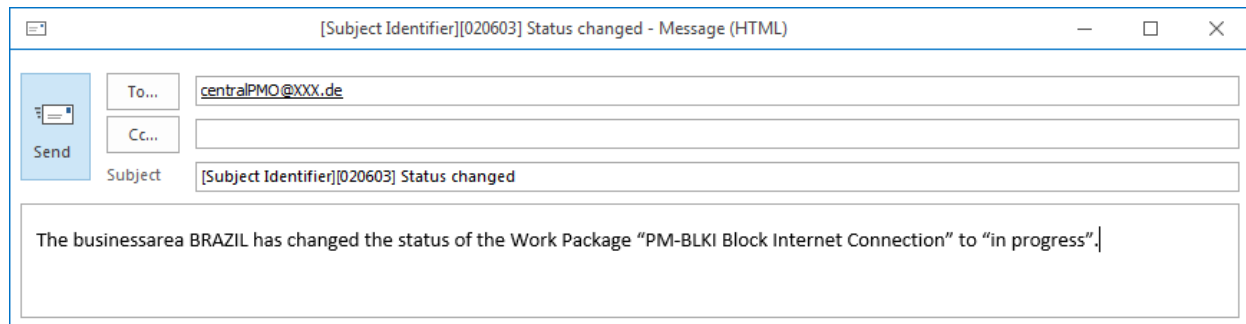
Please update the information using the status links provided in the table below.

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:



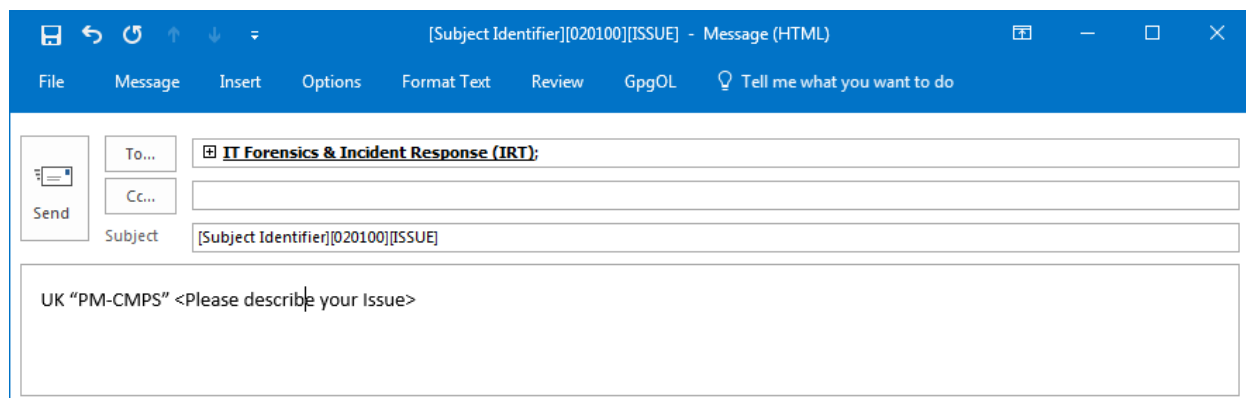
Click on 'Send' to send the response mail.

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

## 2.3 Report Issue

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

A new message window will pop up:



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