Crisis management procedure

Last updated by: 13-09-2022

Owner of the document: Crisis Management Team
Responsible Executive Member: REMOVED

REDACTED PUBLIC COPY

In this document all names, e-mail addresses, examples, metadata and links to files and internal environments have been replaced by 'REMOVED'. This redacted copy has been reviewed by the Crisis Management Team on 28-09-2022 and may be shared with (potential) customers.

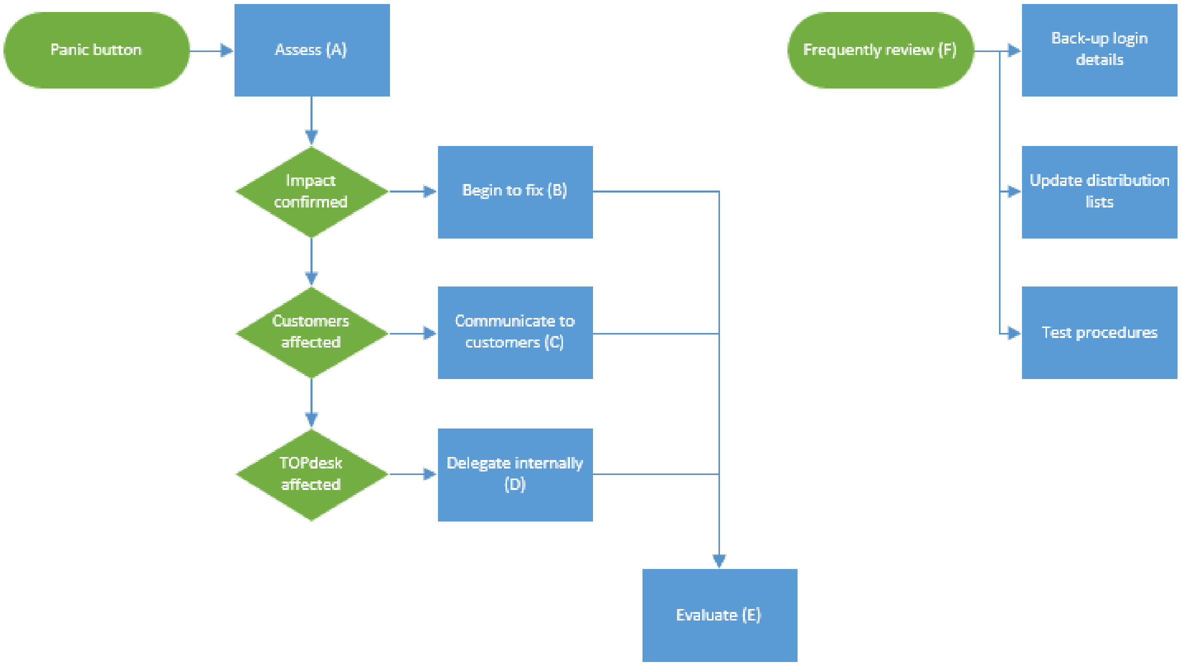
TOPdesk

Contents

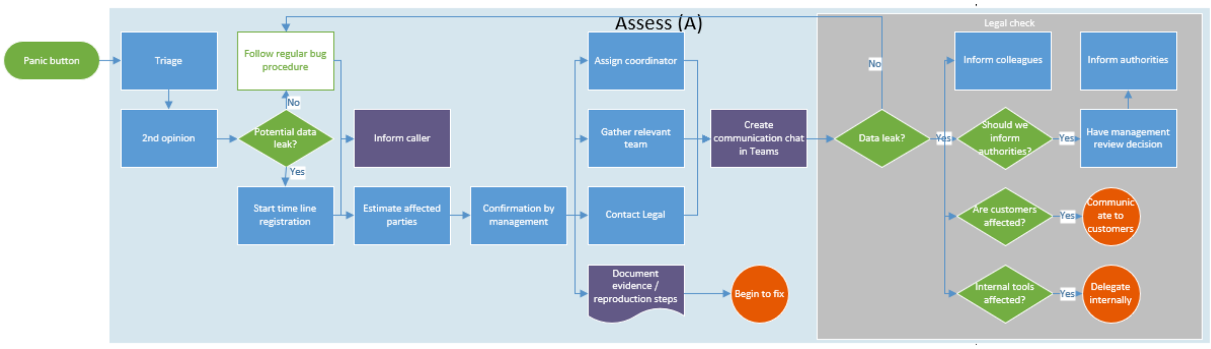
Crisis management procedure - Summary

The crisis management procedure can consist of several phases:

- Assess (A)
- Begin to Fix (B)
- Communicate to Customers (C)
- Delegate Internally (D)
- Evaluate (E)
- Frequent Review (F)



Assess (A)



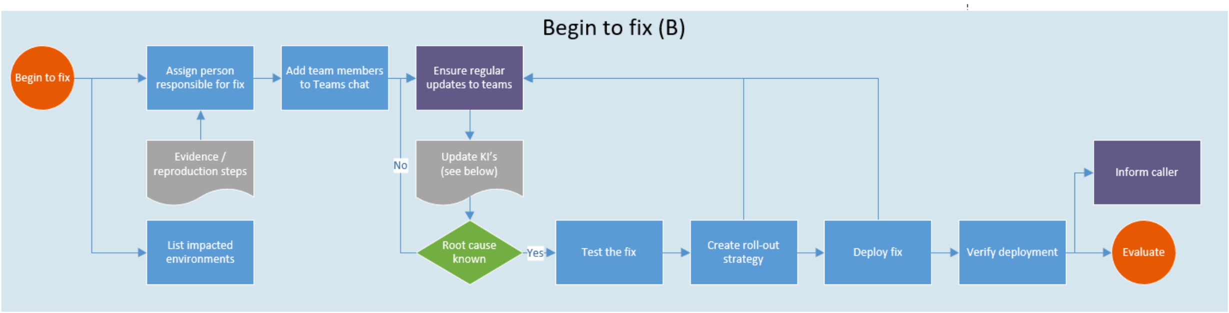
When working on these steps, remember this is intended to provide the team with a QUICK assessment of the situation. In depth checks and reviews will be done in later stages. The whole Assess phase should take at most a few hours.

1. Panic button: The panic button has been used, a new incident has been registered and a message appeared in the "CMT- Crisis Management Team" REMOVED channel.
2. Triage: The first responder does a check to see if this is a valid case to go through the crisis management procedure. Adjust the status to 'being processed' and assign to yourself (so no additional actions are triggered automatically).
3. 2nd opinion: the first responder asks another member of the Crisis Management Team (CMT) to check if they agree with the triage decision.
4. Potential data leak: When both members of the CMT team agree this is a potential data leak, we continue with the investigation. If not, the issue should be resolved using our regular procedures at Support/IT/etc. The CMT will advise the caller on how to continue.
5. Start timeline registration: The decision made in the initial triage and the 2nd opinion are documented in the incident in REMOVED (by the first responder).
6. Inform caller: The first responder sends a first response to the caller, so he/she knows we are investigating. See Template C12
7. Estimate affected parties: The first responder makes an estimate of the affected parties: who is affected, how many colleagues, how many customers, what is the impact for them, etc.
   This estimate is included in the timeline.
8. Confirmation by management: The first responder asks for confirmation by management to follow the crisis management procedure:
   a. In case it's affecting only one branch, ask the branch manager
   b. In all other cases, ask a member of the Executive team.
9. First responder assigns a coordinator (should be someone who has done a training in the last year).

10. Gather relevant team: the coordinator gathers relevant team of the poole of people who have done the training in the last year: Minimum 3, max 5 (inc. coordinator). And it’s made clear which member is responsible for what:
    a. Begin to Fix (B) – called the B-responsible
    b. Communication towards customers (C) – called the C-responsible and
    c. Delegate internally (D) – called the D-responsible.
    d. Evaluation (E) is arranged by the coordinator.
    e. This team will be called the ‘crisis management team of this situation’.
11. Contact Legal: The Coordinator informs legal that there is a crisis situation and asks for an available representative.
12. Legal check
    a. Is it a potential data leak? The Coordinator presents the issue and the documented evidence to the Legal representative to verify if we are indeed dealing with a data leak. Make sure all below issues are discussed and that the decision is registered in the timeline.
    b. Do we inform authorities? The Coordinator contacts legal to review if we should inform the authorities.
        i. If so, have management review decision: ask for confirmation by management to inform authorities:
            1. In case it’s affecting only one branch, ask the branch manager
            2. In all other cases, ask a member of the Executive team.
        ii. If we have to inform the authorities, decide who will deal with that.
    c. When customer data is affected, continue with the steps to communicate to customers
    d. When internal tools are affected, continue with the steps to delegate internal communication
13. Document evidence/reproduction steps: This must be included in the timeline in REMOVED. This is the coordinators responsibility.
    a. Once the reproduction steps are clear we can start to fix the issue. Continue with the steps to begin to fix the problem.
14. Create communication chat in REMOVED:
    a. The coordinator starts a REMOVED chat with the team members.
    b. This chat should have a name that indicates this crisis situation.
    c. This chat starts with a message, based on Template C8.
    d. This first message needs to be pinned! So everyone added later on always sees this.
15. The Coordinator creates a second REMOVED chat to gather important decisions and daily summaries only, the so called ‘timeline’. The coordinator ensures this is updated regularly. Make sure a link to this timeline is added to the first post of the general chat.

16. Inform colleagues: The coordinator informs contact persons in branches, that we are starting the crisis situation procedure (email template C3).

Begin to Fix (B)



When working on these steps, please make sure important events (like the result of each step) are mentioned in the 'Timeline' chat that was created by the Coordinator (see A.15).

1. Assign person responsible for fix: The B-responsible finds a person responsible for creating the fix. Depending on the problem this could be anyone from SaaS Operations to IT to FM.
   In case you need to find someone at development and cannot decide who, based on REMOVED, contact the Development Leadership team (DLT), and they will find the right person/team for you.
   a. The B-responsible makes sure the Evidence and/or reproduction steps are known to the 'person responsible for fix'.
   b. The B-responsible adds the 'person responsible for fix' to the REMOVED chat.
   c. The B-responsible explains the responsibilities of the 'person responsible for fix': The person responsible for fix is responsible for creating the fix, if external parties are needed, escalation is needed, etc, it's the responsibility of this person to get approval for that, arrange it, etc.
2. List impacted environments: When a subset of customers is affected, the B-responsible finds a person that will create a query to determine affected customer environments. SaaS Operations or SaaS Support can run the query across SaaS environments (see step C.9). When creating the query, the person creating the list should keep in mind that:
   a. Usage data for services is stored in separate databases. When you need this data to determine who's affected, contact the Development team responsible for that service to ensure you use the right data model for that database.
   b. Customers might use older TOPdesk versions, resulting in them using different API versions and/or different service versions than the most recent one.
   c. Some (REMOVED) customers have opted out of storing usage metrics, which might affect your options to detect the issue. In those cases, assume they are affected.

3. The ‘person responsible for fix’ might conclude that to mitigate the damage it’s helpful to temporarily shut down a service, application, or SaaS environment. In those cases, check the ‘kill switch mandate’ in appendix B3 for a list of persons that can authorise the shut down of certain services.
4. The ‘person responsible for fix’ is also responsible for regular communication towards the crisis management team of this situation:
    a. Add team members to REMOVED chat: The found ‘person responsible for fix’ adds the relevant colleagues working on the fix to the REMOVED chat. For example, product managers, developer or other colleagues.
    b. Ensure regular update to REMOVED: The ‘person responsible for fix’ will make sure regular updates are given in the REMOVED channel so everyone is aware of the current state and to keep the timeline up to date.
    c. The ‘responsible for fix’ makes sure the C-responsible has enough information to update/create KI’s when more is known about the fix, the rollout, or the implementation.
5. When creating and deploying a fix, don’t forget to:
    a. Test the fix: Ensure the original reproduction steps are no longer possible when the fix is deployed, and that the fix itself does not cause additional problems (aka, test the fix).
    b. Create roll-out strategy: The ‘person responsible for fix’ will make sure a roll-out strategy is created. Involve others (IT, SaaS, Release management, …) where necessary. When creating the roll-out strategy consider the following groups:
        i. SaaS customers with Continuous Deployment
        ii. SaaS customers with infrequent updates
        iii. SaaS customers that have opted out of storing metrics (REMOVED)
        iv. On Premises customers (Virtual Appliance)
        v. On Premises customers (Classic) – End of life
    c. Deploy fix: the ‘responsible person for fix’ will make sure the fix is rolled out and the REMOVED chat is updated. Ensure the release coordinator is involved.
       For patches, please check this procedure.
    d. Verify deployment: The ‘person responsible for fix’ makes sure the fix is deployed successfully to all affected customers, and the REMOVED chat is updated.
6. If all is well, the caller of the ticket is updated with the status by the coordinator.

Communicate to Customers (C)

When working on these steps, please make sure important events (like the result of each step) are mentioned in the 'Timeline' chat that was created by the Coordinator (see A.15).

Two types of issues are considered for Communicating to customers:

1) *Issues requiring immediate communication (within minutes), for example when the network is down, and customers cannot reach us in any way.*
2) *Issues where there is some time to prepare a message (within hours), like security/privacy/data leak type of issues.*

Steps for issues that requires immediate communication (within minutes)

When customers cannot reach us, or colleagues cannot reach each other, due to network failure, phone line failure, etc. the following steps can be taken, depending on what is and isn't working.

Alternatives for when the phone lines aren't working can be found in Template B.5

This list is showing possible communication options, decide per situation what is useful!

1. Depending on the situation, the following options are available to inform **customers** immediately (in order of desirability):
   a. **A news item on REMOVED**
      i. What/when: this only works when REMOVED/REMOVED is available for customers.
      ii. How: Create a news item yourself or ask a supporter to do so.
      iii. Remarks: The news item should be made in English, available for all customers. You can contact translators (see Appendix C5) when needed or ask Support colleagues to translate.
   b. **A news item on our Status page (status.topdesk.com)**
      i. What/when: When REMOVED/REMOVED is not available to customers, or when customers may notice a disruption in one of our services (phone systems unavailable, mail server malfunctions, etc)
      ii. How:
         1. You can publish a disruption affecting TOPdesk SaaS hosting locations from REMOVED / REMOVED using the context menu action as described on REMOVED
         2. If the standard action cannot be used, contact one of the people with Status page access (see appendix B4) to manually publish a message.

iii. Remarks: For each manual post/update/change on the Status page, check if you want to inform subscribers. By default this option is checked for all changes, which can result in spam.

c. A news item/banner item on the website

i. What/When: This only works if the website is available!

ii. How: Ask .... To publish a statement...

d. Via social media channels

i. What/when: when we have no other means than the socials to inform customers, or when we expect customers to reach out via socials for further questions.

i. How: Reach out to team REMOVED, by email with the term 'urgent' in the title.

ii. How: ask them to maintain the NL socials and ask them to setup messages for other branches to publish them and make other branches aware of this.

2. Depending on the situation, the following options are available to inform **colleagues** immediately (in order of desirability):

a. An email to REMOVED (aka REMOVED)

i. What/When: Can be used to reach all colleagues when e-mail systems are working. Note that the use of this e-mail group requires permission from IT.

ii. How: Use Template C7 for inspiration

iii. How: Include a 'spread the word' message.

b. A news item on REMOVED

i. What/When: This only works when REMOVED is available

ii. How: Use Template C7 for inspiration

iii. How: Include a 'spread the word' message.

c. The "TOPdesk Crisis Management" REMOVED chat

i. Who: Managing Directors, Executive team members and the Crisis Management Team are part of the REMOVED chat group 'TOPdesk Crisis Management'

ii. When: This chat group can be used in case of infrastructure outage or other situations where the Crisis Management Team (CMT) or IT cannot immediately be reached by conventional means (such as the panic button), especially in situations that require immediate assessment by the CMT or IT

iii. How: Use Template C7 for inspiration

iv. How: ask them to:

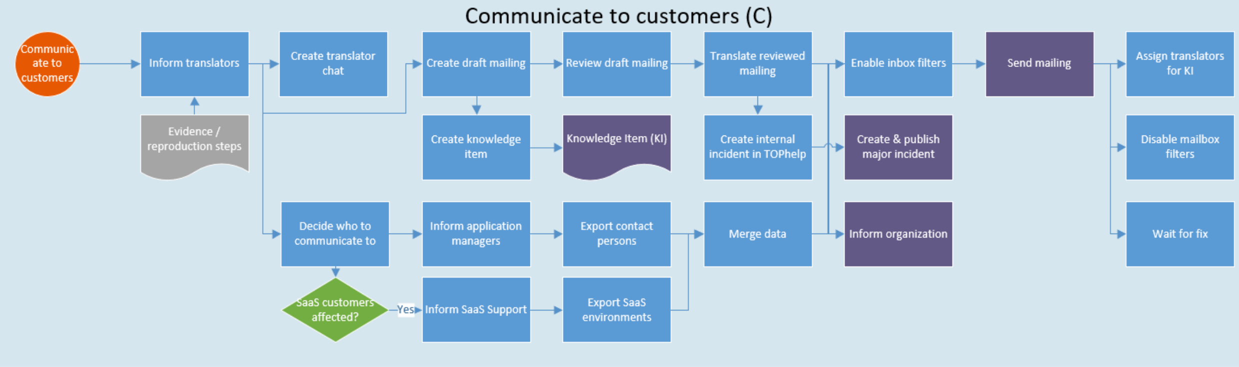
- spread the news in their own branch and REMOVED.

- make sure those who are maintaining the socials are aware of the situation and act on customer reactions.

d. **The "TOPdesk Crisis Management" REMOVED group**
   i. What/When: Using this group should be a last resort!
   ii. Who: Managing Directors, Executive team members and the Crisis Management Team are part of a REMOVED group which can be used when all other options mentioned above are no longer available.
   iii. How: Use Template C7 for inspiration
   iv. How: ask them to spread the news in their own branch and REMOVED, make sure those who are checking the socials are not left out! (Customers will reach out via socials, when we cannot be reached in the normal ways)

3. Wait for the fix:
   a. The C-responsible will wait for the fix and makes sure new relevant information is shared with customers and/or colleagues.
   b. In case it's taking longer (hours) do check if preparing an email message to customers is valuable, if so, follow the steps below to prepare a message. (this is only an option when you can email! You could consider working on a text already, for when mail is working again later, to explain the situation).

Steps for issues where some time is available to prepare a message (within hours)



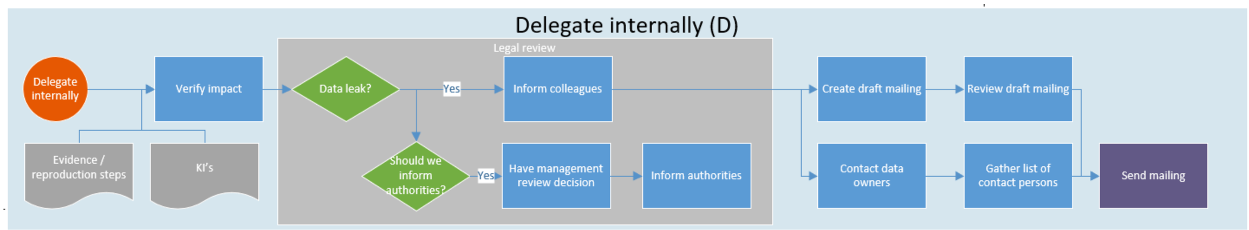
1. Inform translators: send the translators a heads-up message that their help is required at some point in the near future (use email template C4). Include when you expect the text to be ready. This should be sent to REMOVED-translators.
2. Create translators chat: When translators respond, add them to a REMOVED chat with the C-responsible and the Coordinator so you can quickly inform them in case changes are required to the e-mail or knowledge item.
3. Decide who to communicate to: The C-responsible will, together with the rest of the crisis team, determine if and which SaaS and/or OP/VA customers need to be informed. Use the list of impacted environments from step B.2
    a. When querying help is needed, to check which customers or operators have a specific set of permissions, Team REMOVED can be reached via their REMOVED channel, escalation path: DLT.
4. Create draft mailing: The C-responsible makes sure a first draft (or multiple drafts in case SaaS and OP/VA needs different messages) are created, based on template C1.
    a. Determine which Category, Affected systems and Severity should be mentioned. The severity depends on how we want the message to be received.
5. Inform application managers: The C-responsible will arrange a REMOVED application manager who can help to export contact persons.
6. Inform SaaS Support: The C-responsible will arrange a SaaS Supporter (REMOVED plan board, +31152700921 or d-saassupport) who can help to extract SaaS environment data. In case of an issue outside office hours, contact the REMOVED standby operator of that day to create the export.
7. Review draft mailing: The C-responsible makes sure at least two persons check the draft of the e-mail that will be sent.
    a. at least one team crisis management member (ideally the coordinator),
    b. a native English speaker (see Appendix D for potential natives), and/or
    c. someone from team REMOVED

    When times are mentioned in the e-mail, always include the time zone.

8. Create knowledge item: The C-responsible makes sure a Knowledge Item (KI) is created, based on template C2.
   When times are mentioned in the KI, always include the time zone.
9. Export data: With the help of the contact persons you found in previous steps, export all necessary data. Use the templates to export data from REMOVED.
   a. Export contact persons: The C-responsible will arrange an export of the contact persons that need to be informed.
      i. For OP/VA customers, this should be a list with active contact person's name, contact persons email, customer unid, preferred language, liftsource, business unit.
      ii. For SaaS customers, this should be a list with active contact person's name, contact persons email, customer unid, preferred language, liftsource, business unit.
   b. Export SaaS environments: The C-responsible will arrange an export of the affected SaaS environments (ts-numbers and unid of customer)
   c. Merge data: The C-responsible will make sure the ts numbers will be merged with the customer data, so we end up with a list of email addresses of those SaaS customers that need to be send.
   d. Make sure all this information is stored in the REMOVED channel -> Documentation previous crisis situations -> Folder for this situation.
10. Translate reviewed mailing: The C-responsible makes sure the translators translate the mailing.
    Use Template C5 for the content of the email.
11. Enable inbox filters: The C-responsible will make sure bounced emails will be processed by a specific filter to prevent loads of unnecessary emails in REMOVED. See KI 15175 in REMOVED for instructions.
    It takes some time for the filters to take effect, so do this at least 15 minutes before step 14 (sending the mailing).
12. Create an internal incident: You need this to create a major incident. It can be used for your own registration or closed once the major is created.
13. Create and publish major incident in REMOVED (from the internal incident)
    a. The C-responsible makes sure a major incident is created in REMOVED. First fill the short description and request field, then publish the major in the SSP. The major is created so customers who have questions regarding the email they received can use this major to register this question. This helps us to keep an overview of the number of questions, and make sure they are properly answered.
    b. The C-responsible makes sure Support is aware of this major ticket, by putting a message on the Support REMOVED Announcement channel, marked important and mentioning '@general'.

14. Inform organization: The C-responsible makes sure all colleagues are informed, via REMOVED and by e-mail (REMOVED). Use Template C7. Note that the use of this e-mail group requires permission from IT.
15. Send mailing: The C-responsible will make sure the email is sent. Use the instructions in ‘How to create crisis communication e-mails in REMOVED’.
    Make sure at least one other colleague reviews the settings before you send out the mailing. Each mailing is checked for:
    a. BCC usage (only applicable when sending manually)
    b. Sender: REMOVED
    c. High Importance: checked on
    d. Working hyperlinks
    e. Correct subject
    f. Signature and TOPdesk logo (only applicable when sending manually)
16. Assign translators for KI: The C-responsible makes sure there are translators to keep the KI up to date.
17. Disable the mailbox filters: The C-responsible makes sure that after 15 minutes of sending the last email the mailbox filters are deactivated. See KI 15175 in REMOVED for instructions.
18. Inform branches which of their customers have been emailed. Use template C6 to update them.
    To avoid sending big lists of customers to everyone, please you can send instructions on how to create a selection, or send a list of affected customers per branch, to the indicated contacts within that branch (Appendix A)!
    a. This list per branch should include at least the contact person’s name, the customer name and the business unit.
19. Make sure the sent e-mail is stored in the REMOVED folder (the folder of this specific crisis situation) so that we can prove to auditors that we informed our customers of this event.
20. Wait for the fix: The C-responsible will wait for the fix and makes sure there are regular progress updates to the KI with new relevant information (in all supported languages).

Delegate Internally (D)

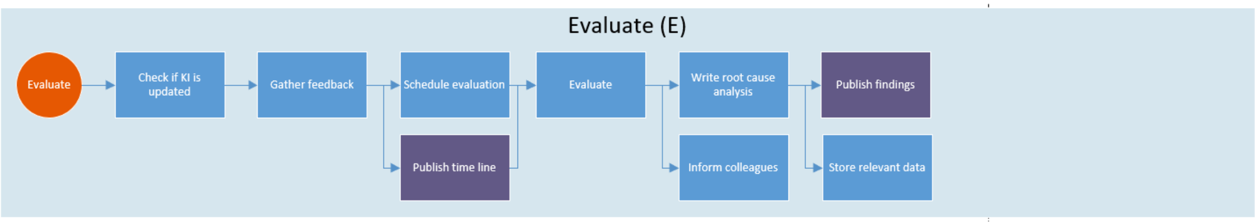


When working on these steps, please make sure important events (like the result of each step) are mentioned in the 'Timeline' chat that was created by the Coordinator (see A.15).

1. Verify impact: The D-responsible verifies with the data owner(s) if TOPdesk is affected.
    a. In REMOVED you can find a list of internal TOPdesk SaaS environments. Also, don't forget about REMOVED itself.
    b. In REMOVED you can find a list of internally used software and it's contact persons in our register of Privacy Impact Assessments.
2. Legal review:
    a. The D-responsible checks if the earlier legal assessment still valid? If not, go through the following steps:
        i. Is it a data leak? The D-responsible contacts legal to review if we are dealing with a data leak.
        ii. Do we inform authorities? The D-responsible contacts legal to review if we should inform the authorities.
        iii. If so, have management review decision: ask for confirmation by management to inform authorities:
            1. In case it's affecting only one branch, ask the branch manager
            2. In all other cases, ask a member of the Executive team.
        iv. If we have to inform the authorities, decide who will deal with that.
3. If we have to inform colleagues:
    a. Create draft mailing: The D-responsible makes sure a first draft is created, based on template C9
    b. Review draft mailing: The D-responsible makes sure at least two persons check the draft, at least one team crisis management member, ideally the coordinator, and someone from the internal communication office.
    c. Contact data owners: D-responsible contacts data owners to get a list of people potentially affected by these issues.
    d. Gather list of contact persons: Get the list of people potentially affected.
    e. Send mailing: send the emails and update the REMOVED chat.
    f. Make sure the sent e-mail is stored in the CMT REMOVED folder so that we can prove to auditors that we informed our colleagues of this event.

4. If we have to inform the authorities
    a. Contact the Data Protection Officer to coordinate all actions
    b. Review the decision to inform authorities with management
        i. In case it’s affecting only one branch, ask the branch manager
        ii. In all other cases, ask a member of the Executive team.
    c. Decide which authorities should be informed. This can differ per country and even per region (notably in Germany)
    d. Gather relevant information (number of affected colleagues, start and end times (see timeline), e-mails sent to colleagues, etc. Similar to template C2
    e. Submit a report to the authorities within 72 hours of finding out internal environments are affected
5. Write a report: Create a report for our internal registration. Use template C10

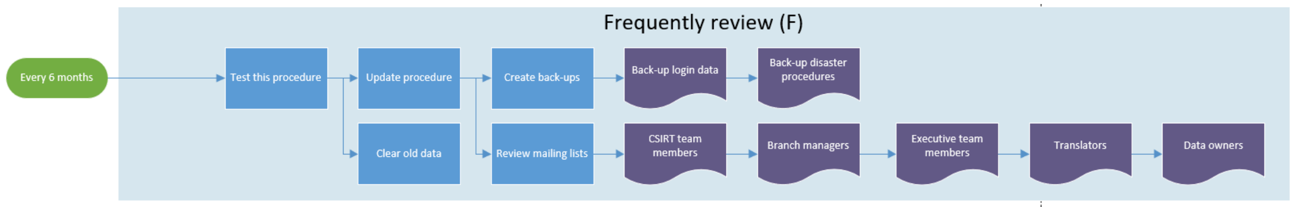
Evaluate (E)



1. Check if KI is updated: The coordinator makes sure all the information is in the KI, including translations.
2. Gather feedback: The coordinator makes sure all involved colleagues (or external parties) are asked to send in feedback and collect this.
3. Schedule an evaluation: The Coordinator schedules an evaluation, which include the following colleagues:
    a. The crisis management team setup for this situation (first responder, B-responsible, C-responsible, D-responsible)
    b. Someone who represents the ‘victims’, who ideally asks why/why/why?
    c. The legal person who was involved
    d. Optional:
        i. Management colleague (optional)
        ii. Communication colleague
        iii. Colleague responsible for the fix
        iv. Colleague responsible for the out roll of the fix
        v. A branch manager or sales/marketing colleague (optional)
        vi. A chair who was not involved in the process
4. Publish a timeline: The coordinator makes sure all information is gathered from the REMOVED chat and ticket(s) to form a complete timeline. This is stored in the “CMT - Crisis Management Team” REMOVED channel.
5. Evaluate: The coordinator makes sure the evaluation meeting is roughly following the following template:
    a. What happened?
    b. What was the cause?
    c. How was it solved?
    d. How can this be prevented?
    e. Was the procedure correctly used and can it be improved?
    f. Was the communication done properly and timely?
    g. Were the stress levels manageable, can we reduce the workload?
    h. Decide, do we need to publish a RCA if so, internally or externally?
6. The Coordinator makes sure minutes of the evaluation are made, use template C11.

7. The Coordinator makes sure, all to-do's that came from the evaluation meeting are stored in the Kanban board 'follow up crisis situations' in the REMOVED. Make sure the label of the tasks is reflecting the date of the situation.
8. Inform colleagues: The coordinator makes sure the advice is communicated to the relevant parties.
9. The Coordinator makes sure a copy of the minutes is posted as update of the Crisis management team on REMOVED.
10. When necessary:
    a. Write root cause analysis: The coordinator makes sure a write up of the evaluation is created, which (depending on the audience) can be published internally or externally. Template C10 can be used to create the RCA.
        i. In case of an externally published RCA; involve communications, marketing, or an experienced Sales colleague.
    b. Publish findings: The coordinator makes sure the RCA is published, this can be done in REMOVED, the SaaS status page, a newsletter, or the website (depending on the situation). REMOVED can help here.
11. Store relevant data: All relevant information should be stored in the folder for this situation, in the REMOVED channel. In that folder, make sure you store:
    a. Timeline
    b. Queries and exports
    c. The mailing texts that were sent, in all languages.
    d. The RCA
    e. The minutes of the Evaluation
    f. Other relevant documents
12. The Coordinator updates the original REMOVED incident:
    a. Copy the text of the evaluation minutes in the Action field.
    b. Adjust the brief description to the format 'Name (procedure followed)', for example: "Possible data leak 2021-01-31 (Procedure followed)
    c. Close the incident.

Frequent Review (F)



1. Test this procedure: When the full procedure has not been used or tested for half a year, want to test the procedure, so everyone knows how to use it. It is the responsibility of the lead of the CMT to arrange this.
2. Update procedure: All the steps in this procedure should be tested and updated where necessary; including KI 2988 on AVG data breach assessment.
3. Clear old data: Clean up data stored in folders for old (>1 year) incidents. Make sure personal data (exported lists of persons) are deleted and old KI's in REMOVED are archived.
4. Review mailing lists: Make sure all contact details used in this procedure are still up to date.
    a. Mailing lists that should be reviewed:
        i. REMOVED
        ii. REMOVED
        iii. Check and update Appendix A together with those mailing lists.
    b. Other lists:
        i. CMT members list in Appendix B
        ii. Check members of the AD group used for exporting contact persons from the report server with IT
        iii. Update pool of people who did the training in the last year
        iv. Board members list in Appendix B
        v. Executive team members list in Appendix B
        vi. Are phone numbers of ET, Board and BM available via REMOVED? (The phone number of REMOVED will not be there on purpose).
        vii. Update REMOVED with relevant people in the General TOPdesk numbers section. (REMOVED maintains the other info).
        viii. List of Native speakers you can contact in Appendix D
        ix. Internal application managers & Internal data owners (WIP 2-3-2022)
        x. Appendix B2 – update the list and adjust the REMOVED chat and REMOVED group accordingly.
        xi. Appendix B4 – update the list of colleagues with Status page access

2. Create backups: Make sure we've got a back-up of the data needed to follow this procedure, even when the TOPdesk network and/or offices are not available. Include at least:

a. Back-up login data (should not depend on TOPdesk network)
    i. status page
    ii. TOPdesk Twitter account (or other social media)
    iii. any tool used for mailings
    iv. TOPdesk.com website REMOVED
b. Back-up disaster procedures: Print/copy most recent version of this procedure and all templates and files in the REMOVED folder
c. And make sure every individual of the Crisis management team stores a copy of this procedure including the templates and files on their (encrypted) work laptop.

Appendix A - Who to inform - split by branch

The people mentioned below, together form the distribution list ‘REMOVED’.
If the “Who to inform – translations” column has the value NA, it means that branch is happy with communicating in English towards customers. This was approved by the managing directors.

Branch	**Who to inform - general**	**Who to inform - translations**
CA	REMOVED	REMOVED
AU		
BE		
BR		
DE		
DK		
HU		
NL		
NO		
UK		
US		
Global		

Appendix B – REMOVED, People and Definitions

Board	REMOVED
Branch managers	REMOVED
REMOVED/REMOVED	The old and the new TOPdesk wide communication platform. REMOVED is expected to be replaced by REMOVED in 2022.
Coordinator	The coordinator • Has an overview of what is happening and the progress, from this start to evaluation. • Assigns roles and responsibilities • Makes sure the timeline is updated properly and complete • The coordinator is the owner of the REMOVED chat. • The coordinator makes sure the REMOVED chat contains the full time line of the crisis situation.
Crisis management team of this situation	The team assembled during a crisis, consisting of the following roles: - Coordinator - B-responsible - C-responsible - D-responsible
Crisis management team (CMT)	The Crisis management team consists of: - REMOVED (lead), - … - REMOVED (Legal representative)
Data leak	This is what the European Commission says about a 'data leak': https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en Possible definition: Any situation where a user has possibly had access to information that that user should not have been able to see. The information must be Personally Identifiable Information.
Executive team	Members can be found on REMOVED
First responder	The operator from the crisis management team that picks up the ticket or answers the person that reports the problem.
KI	Knowledge item; an article within the TOPdesk software with information for the affected end users.
Major incident	The method within the TOPdesk software to collect tickets with a similar cause.
Panic button	The button on REMOVED, REMOVED and REMOVED to reach the Crisis Management Team.

Poole of people who did the training in the last year	Next to the members of the crisis management team, the following people can help out during a crisis situation: - REMOVED
RCA	Root Cause Analysis (see Appendix C10)
REMOVED	The TOPdesk instance for TOPdesk employees to contact customers.
Timeline	The timeline gives a thorough view of what has been done, when and by who. It should include at least: • The actions taken • Decisions made, including who were involved and who made the final decision • Daily summaries.
Ts-number	The unique identifier for all SaaS environments.
Unid of customer	A system field for the unique values for each customer in the REMOVED system

Appendix B1 – Emergency contact list

Besides the emergency contact list as provided for mostly SaaS & IT purposes on the Wiki (see: REMOVED, requires access to the internal network or the paper version), there is a list of emergency contacts based on them being able to assist within their field. The people mentioned here have agreed to “drop everything they're doing” and to assist the CMT when contacted during office hours as part of this procedure.

Development	REMOVED
IT & Internal infra	
Social media	
Web & hosting	
Customer Solutions (CS) & Testing (TST)	

Appendix B2 – Which roles should be part of the TOPdesk Crisis management REMOVED group & REMOVED chat?

There is a REMOVED group called ‘TOPdesk Crisis Management’, which serves as a backup means of communication, which can be used in case of infrastructure outage or other situations where the Crisis Management Team/ SaaS / IT cannot be reached immediately by conventional means (such as REMOVED), especially in situations that require immediate assessment by either department. A REMOVED Chat with a similar purpose is also in place, with the same members.

Colleagues with certain roles should be included in those REMOVED group and REMOVED chat. Below you can find the roles, and the current people who fulfil these roles. With the exception of CMT members, all persons below can be found on the REMOVED

Role	**Who**
MD Australia	REMOVED
MD Belgium	
MD Brazil	
MD Canada	
MD Denmark	
MD Germany	
MD Hungary	
MD Netherlands	
MD Norway	
MD United Kingdom	
MD United States of America	
Crisis management team members	
REMOVED / SaaS Operations (minimum 2 persons)	
DE IT	
PO’s IT	
Executive team	
Board	

Appendix B3 – Kill switch mandate

During an emergency we may need to decide to shut down services, disable network connections, or make services unavailable to all or certain users. When the technical experts investigating the disruption (A-responsible or B-responsible) conclude that (temporarily) disabling a service is the best short-term solution, they can verify that decision with one of the mandated groups listed below. Anyone in the mandated groups can allow the technical experts to disable a service.

This mandate for groups that are allowed to decide to disable services has been reviewed with, and was approved by, the CEO on 15-08-2022.

Application/service description	**Mandated groups for decision to disable**
Internal applications only used in one country (example: Lift NL, REMOVED)	Talent leads from that country, Branch manager for that country, Executive team, Board members
Internal applications used internationally (example: REMOVED, mail servers)	Executive team, Board members
Individual TOPdesk SaaS environments	SaaS main contact persons at the affected customer (written confirmation), SaaS Operations members, Talent leads at Support, Branch manager for that country, Executive team, Board members
All SaaS environments in one country (example: environments for Canadian customers)	Branch manager for that country, Executive team, Board members
All SaaS environments or several environments in multiple countries	Executive team, Board members

Note that this list is an example of who is mandated to decide in which situations. It does not, and will never, cover all situations that can occur. Use this list as a guideline to decide on who to consult with, and always use your own best judgement. When in doubt about 2 options, choose the smaller group of mandated people.

Appendix B4 – Colleagues with Status page access

These colleagues can manually update the TOPdesk Status page to edit existing messages and post updates. They can publish disruptions when the link with REMOVED is unavailable due to a disruption.

REMOVED

This list was last updated on 05-09-2022.

Appendix B5 – Delft backup telephony options

In case the TOPdesk Delft main telephone number becomes unavailable due to a hardware issue or power outage on our end, then our provider will automatically reroute incoming calls to a backup number that is outside of our regular infrastructure. Our customers will not notice this and can keep calling our normal number; except for the fact that direct calls to Support will reach the main line tape instead.

In this case, on our end, we can process incoming calls as usual, however outgoing calls via the REMOVED telephony service will not be possible.

The number of this backup line is **REMOVED**, it can also be used as an alternative for the main number if required.

If landlines aren't available at all, but SIP is still operational, then we can still be called on any TOPdesk associated SIP address, however they can be unsuitable for communication due to how it looks and how they are generally attached to individual employees. The alternative is the elegant address attached to the backup line which can be called via any SIP client (such as REMOVED) to reach it, namely: REMOVED

In emergencies such as extended telephony downtime, **REMOVED** can be communicated on the TOPdesk main website as well as the SaaS support page.

More information can be found in REMOVED KI 3104.

Appendix C - Template texts

The templates below show what the structure of those messages should be. The red part should be adjusted to the current situation. It's there to give an idea of what it could look like.
The bold sentences are there to structure the text and make it easier to read.

Appendix C1 – Template draft email to customers

Subject: [brief description of situation]

High Importance: checked on

TO: customers (BCC!!)

Body:

REMOVED

[Note: The sent e-mails (including recipients) must be stored in the REMOVED folder, so we can prove to auditors that we informed our customers. The e-mails must be stored for 1 year, so they are available during the next audit.]

Appendix C2 – Template KI

[NOTE – In case of a data leak, customers must be able to inform their privacy authority about:

- *What happened? The type of issue, a time line, and whether the issue is now resolved.*
- *How many people were affected, and from which countries?*
- *Which categories of data were stored?*
- *Potential consequences to affected persons*
- *Actions that were taken to prevent what happened, and to reduce the consequences]*

REMOVED

Appendix C3 – Template mail to BM and CP's when the procedure starts

Subject: REMOVED

High Importance: checked on

TO: REMOVED (TO, so everyone can see who else from their branch received the email)

Body:

REMOVED

Appendix C4 – Template email towards translators - expect soon something

Subject: REMOVED

High Importance: checked on

TO: REMOVED-translators

(use TO, so everyone can see who else from their branch received the email)

Body:

REMOVED

Appendix C5 – Template email towards translators – to ask for translation

Subject: REMOVED

High Importance: checked on

TO: REMOVED-translators (TO, so everyone can see who else from their branch received the email)

Body:

REMOVED

Appendix C6 – Template email towards BM and other CP's - with emailed customers

Remark for C-responsible: To avoid sending big lists of customers to everyone, please send a list of affected customers per branch, to the indicated contacts within that branch!

Subject: REMOVED

High Importance: checked off

To: all contacts indicated from a specific branch

Body:

REMOVED

Appendix C7 – Template post to inform organisation

Subject: REMOVED

REMOVED

Appendix C8 – Template first Chat message

This chat is used as the log of crisis situation [name that indicates crisis situation].

The situation

[a general description of the situation]

Affected parties

[describe the estimated affected parties]

Evidence/reproduction recipe

[describe the reproduction steps are other evidence of the situation]

The team handling this crisis situation

Management member who confirmed to follow the crisis management procedure: [name]

The crisis management team for this situations consist of:

- Coordinator (of this crisis situation): [name]
- B-responsible (responsible for the Begin to fix part of the procedure): [name]
- C-responsible (responsible for communication towards customers): [name]
- D-responsible (responsible for delegating internally/communicate towards colleagues): [name]

The DO's and DON'Ts of this chat

DO'S:

- Include all actions taken, decisions, chats and updates in this chat.
- When in doubt, just add it.

DON'TS:

- DO NOT start separate chats with other groups, but add people to this chat instead, so there is one timeline with all relevant information.

Appendix C9 – Template draft email towards colleagues

Subject: REMOVED

High Importance: checked on

TO: **REMOVED**

REMOVED

Appendix C10 – Template Root Cause Analysis

Root Cause Analysis (RCA)
<title>

Date:
Present:
Minute taker:
Notes:

Link to REMOVED:
Link to REMOVED:
Link(s) to REMOVED chat(s)/channel(s):

Timeline and actions taken

2024-01-01 11:00	Event 1
2024-01-01 11:00	Action 1

Root cause

Give a summary of what went wrong.

Mitigation steps/procedure

What was done to remedy / repair the situation?

Procedure points of improvement

Points of improvement for the crisis procedure

Communication points of improvement

Points of improvement for communication (internally and externally)

Prevention

What can be done to prevent a comparable situation from happening?

Follow up actions

Who needs to do what?

What now?

Communicate the RCA to relevant parties.
Assign follow up actions to specific persons or REMOVED, state the priority / urgency.
Save the RCA to the Crisis team backups.

Appendix C11 – Template Minutes Crisis situation

Minutes Crisis situation [fill in name/date of situation]

Present

Date:
Present:
Minutes by:

Summary of the situation

REMOVED

Relevant information

[links to KI, Incident, etc.]

Steps taken to resolve the problem

The timeline and actions taken can be found [INCLUDE LINK TO TIMELINE DOC]

Root cause

....

Points of improvements

Points of improvement - Procedure

.....

Points of improvement – Communication/Collaboration

.....

Points of improvement – TOPdesk product

.....

Points of improvement – Other

.....

Appendix C12 – Template text to notify caller

Template text investigation started:

Thank you for contacting the Crisis Management Team regarding this issue. We've concluded our initial assessment of the case and concluded that a full investigation is necessary. The investigation will start now.

We may not be able to keep you updated of all the steps taken, but we'll do our best to keep you in REMOVED. You can expect a more detailed response within a few days.

Template text no full investigation:

Thank you for contacting the Crisis Management Team regarding this issue. We've concluded our initial assessment of the case and concluded that this issue does not warrant an escalation and full investigation by the Crisis Management Team.

To get this issue resolved, we recommend that you [add steps]

Appendix D – Native speakers you can contact

Emails towards customers should be double checked by native speakers. To verify an English email, you can ask for example:

- REMOVED

Appendix E – FAQ

What if translators don’t send their translation in time?

Translators receive an email upfront that their time is needed somewhere in the near future. When a text is available to translate, this is sent to the translators, including a deadline.
If the translation has not been received by that deadline. The customers who preferred communication in that language, will receive the message in English.

What if a branch wants to send a message in their own language later on?

If translations are not made on time, the customers will receive communication in English. If a branch wants to send that same message at a later time in their own language, that’s up to the branch to arrange. The crisis management team of this situation will not send this. However, they can provide a list of recipients of the original mail.

How can I contact management by phone?

Via REMOVED the phone numbers of Board members, ET members and Managing Directors can be found. The numbers can also be found in the REMOVED

Appendix F – Change log of the procedure

Date of change	What changed, including motivation	Changed by
01-04-2022	Removed the name “CSIRT” from the document and made a proper distinction between the “crisis management team” and “the crisis management team for a specific situation”	REMOVED
01-04-2022	Added “poole of people who have done the training in the last year” to appendix B. Included REMOVED	
01-04-2022	Added Appendix C10 (template RCA), including reference to it from the Evaluation chapter.	
4-4-2022	Adjusted “… stores a copy of this procedure including the templates and files on an encrypted USB drive” to “…their (encrypted) work laptop”.	
5-4-2022	Created a REMOVED public copy of the document and added a warning about version control on the first page	
22-4-2022	Added a note that sent e-mails should be stored for 1 year to prove to auditors that we informed our customers.	
3-5-2022	Added to the Frequently review part, to check the Emergency contact list on the wiki	
9-5-2022	Legal check in Assess part has been moved up.	
9-5-2022	The B-responsible was in some cases called ‘Coordinator’ in the Begin to fix section, this has been corrected.	
9-5-2022	The list bullets have been replaced by numbering, for easier reference	
9-5-2022	In the Communicate to customers section, it has been added that you have to create the major, based on the internal incident created.	
9-5-2022	In the Communicate to customers section, the saving emails point has been moved to the end.	
9-5-2022	The Delegate Internally part has been restructured, to make it more clear	
9-5-2022	The task to safe guard the sent emails have been added	
9-5-2022	Added to Communicate to customers setion: Make sure all this information is stored in the REMOVED channel -> Documentation previous crisis situations -> Folder for this situation.	
9-5-2022	In internal templates, you can use the “TO” instead of CC.	
9-5-2022	Added the right distribution list to template C5	
10-5-2022	Added ‘roll-out strategy for On Premises customers’ in the Begin to fix section	

11-5-2022	Add a link to the Emergency Contact list to the FAQ ‘how to contact management’	
11-5-2022	Added making and storing evaluation minutes to the Evaluation step.	
11-5-2022	Added a step to the Evaluation, to add to do’s to the Follow up crisis situation Kanban board	
11-5-2022	Added Template for Minutes (Appendix C11)	
11-5-2022	Add ‘responsible for fix’ to the chat has been added in the B section	
11-5-2022	In the b section, it’s made clear that the B-responsible has to explain the responsibilities of the ‘person responsible for fix’ to that person	
23-5-2022	Updated the procedure according to the feedback at our evaluation on 12-5-2022. Change summary: • Added step to gather a list of affected customers, • added deployment groups for release process, • added timing to mail filter step, • updated steps to inform all colleagues, • added default text about translations to C-1, • added lists of internal environments and software, • moved task for creating internal incident	
25-5-2022	Updated the procedure according to agreement with DLT. When someone is needed from development, and you cannot figure out who, based on REMOVED, contact DLT to find the right person/team for you	
31-5-2022	Updated list of team members in Appendix B	
2-6-2022	Added Publish RCA topic to evaluation meeting format.	
2-6-2022	Added closure of initial REMOVED incident	
3-6-2022	Expanded steps D3-D5 with more details	
8-6-2022	Added more details to step of updating emergency list	
8-6-2022	Added escalation path REMOVED and DLT	
16-6-2022	Added step in Evaluate to publish Evaluation Minutes	
22-6-2022	Updated template C2 so that it better matches the requirements of the Dutch Privacy Authority	
20-7-2022	Made Appendix A clearer by adding text about the preferred language	
20-7-2022	Removed REMOVED as a Danish translator (he left)	
20-7-2022	Added Appendix B2 to specify roles that should have access to the Calamity group	
20-7-2022	Added Frequent review of Appendix B2	

3-8-2022	Added to C: Steps for issues that requires immediate communication (within minutes)	
3-8-2022	Added links to templates/appendix references	
4-8-2022	Expanded REMOVED group membership description	
16-8-2022	Add REMOVED Chat check-up to group membership check	
17-8-2022	Added kill switch mandate to step B.3 and in appendix B3	
30-8-2022	Added CS & TST to emergency contacts	
05-9-2022	Updated Status page access list and kill switch mandate text	
05-9-2022	Updated template C4	
05-9-2022	Added template C12	
8-9-2022	Added parts about the Socials in section C	
13-9-2022	Added appendix B5, on Delft office backup telephony, requires rephrasing for use as a template (and move to C)	