Incident Response Management Handbook

Document Information

Version:	1.1
Datum:	07. Jul. 2021
Status:	Final
Author:	Samuel Mühlebach, CISO Fides Treasury Services AG
Classification:	Intern

Content

1 Goals

The incident response management handbook of Fides Treasury Services AG (FTS) documents the process and instructions to be followed in the event of an incident.

2 Scope

The incident response management handbook is binding for all units and all employees of FTS.

3 Incident response management organization

Following, the permanent and ad hoc members of the incident response management organization are listed including their role and responsibilities.

3.1 Permanent members

Role	Name	Role and responsibility
Incident response manager	Dos Santos, Edar +41 79 238 6049	Decides on the classification of events, immediate measures, incident response management measures and any escalation to crisis management.
Chief information security officer (CISO)	Mühlebach, Samuel +41 78 889 6700	Recommends measures to ensure information security.
IT service desk	IT support +41 79 944 5062	Single point of contact, confirmation of the message, initial entry in the incident response management logbook, information about the event on the FTS intranet.
Business applications	Roman Müller +41 79 655 1915	Decides on measures affecting business applications.
User services	Niki Hausammann +41 78 860 4200	Decides on measures affecting user services.
Infrastructure	Niki Hausammann +41 78 860 4200	Decides on measures affecting the infrastructure.

Role	Name	Role and responsibility
CIO	Bernhard Kaiser +41 78 750 41 99	Will be directly informed by the incident response manager but plays no active role.

Table 1: Permanent members of the incident response management organization

3.2 Ad hoc members

Role	Name	Role and responsibility
Representatives of the external IT service providers	Niki Hausammann +41 78 860 4200	Will be consulted if a service is affected by an external IT service provider (e.g. network operation by Swisscom).
Human resource department	Philipp Gysi +41 79 460 7915	Will be consulted if personal data is involved (e.g. unauthorized access, unauthorized disclosure).
Legal and compliance department	Jan Hugelshofer +41 78 631 0154	Will be consulted in case of violation of applicable law.
Data protection officer (DPO)	Roman Müller +41 79 655 1915	Will be consulted if personal data is involved (e.g. unauthorized access, unauthorized disclosure).
Media relations and corporate communications	Media Hotline +41 844 33 88 44	Will be consulted if the public and the media need to be informed.
Facility management	Niki Hausammann +41 78 860 4200	Will be called in if buildings or operations are affected by the IT emergency.
Computer security incident response team (CSIRT)	Wagner, Robert +41 79 7955638 Halter, Ralph (A) +41 79 6233451 Richner, Christoph (A) +41 79 5007828	Is called in to support the IT Security Officer in the event of cyber attacks and to assist the Legal Department in the preservation of evidence and investigations (e.g. in cases of suspected fraud).

Table 2: Ad hoc members of the incident response management organization

3.3 RACI Matrix

The RACI matrix regulates the responsibilities of the entire incident response management process.

R - Responsible: responsible for the execution of the task

A - Accountable: bears responsibility, is accountable and makes decisions about costs, risks, etc.

C - Consulted: must be consulted (e.g. technical expert)

I - Informed: must be informed

Activity	Messenger	IT service desk	Incident response manager	Information security officer	System owner	Crisis management team
1. incident logging	C	R	A			
2. confirmation	I	R	A	I		
3. classification	I		A, R	C		I
4. immediate measures	I		A	C	R	
5. recovery	I		A	C	R	
6. confirmation of normal operation	I		A, R	I		I
7. post-mortem analysis			A		R	I

Table 3: RACI matrix

3.4 Overarching organization

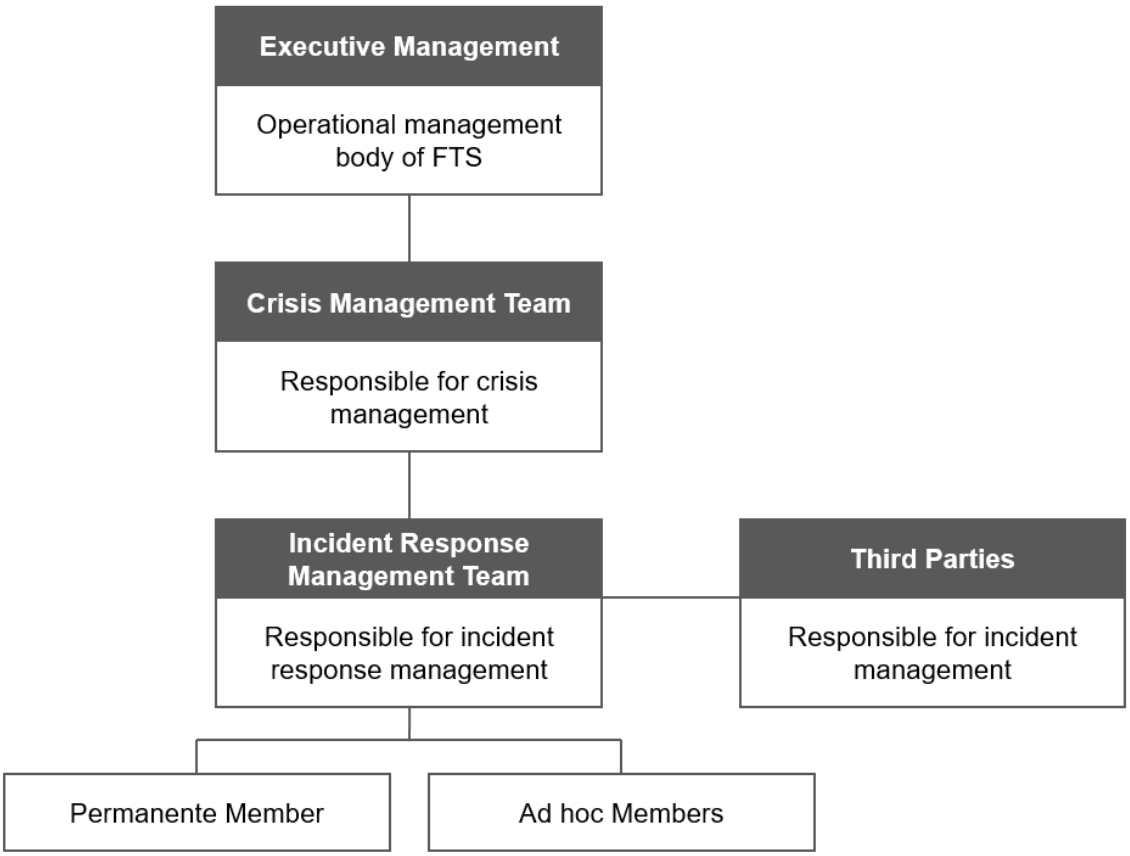

Figure 1: Overall organization

Incidents, major incidents, and crises are managed at the appropriate organizational level. This ensures short decision-making processes and immediate reaction. If necessary, incident or major incidents can be escalated to the next higher level.

4 Incident response management phases

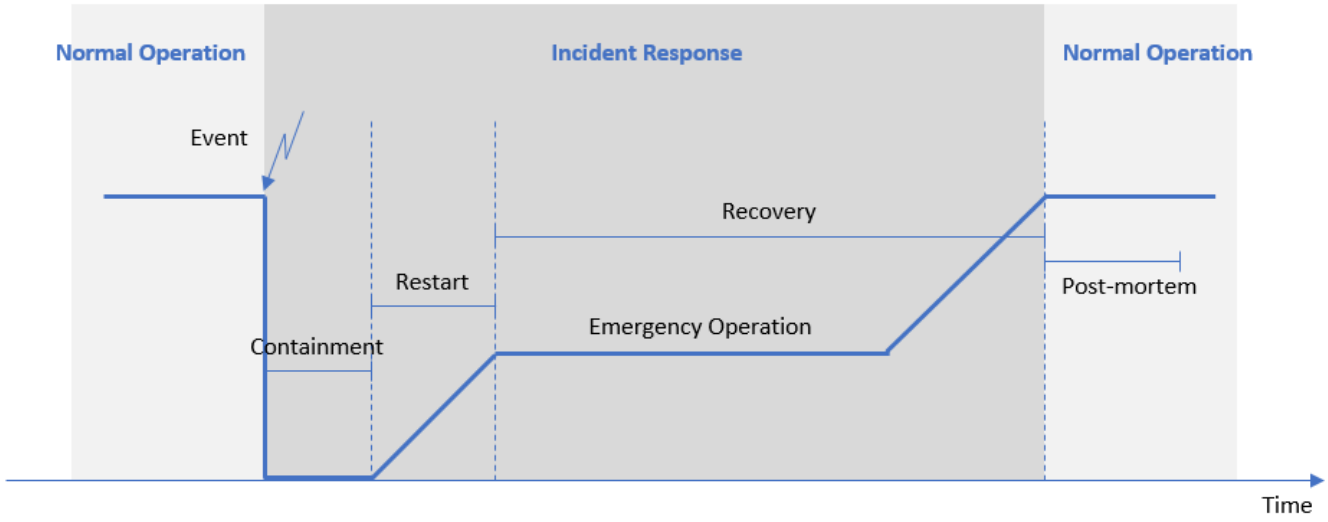

Figure 2: Phases of incident response management

The occurrence of an event triggers the emergency management process. The first stage of the incident response process is the proper identification and confirmation of the event. The second stage is the containment to limit the impact of the incident. The third state is the restart of the emergency operation. And finally, as fourth step the recovery to normal operation.

5 Incident Response Management Process

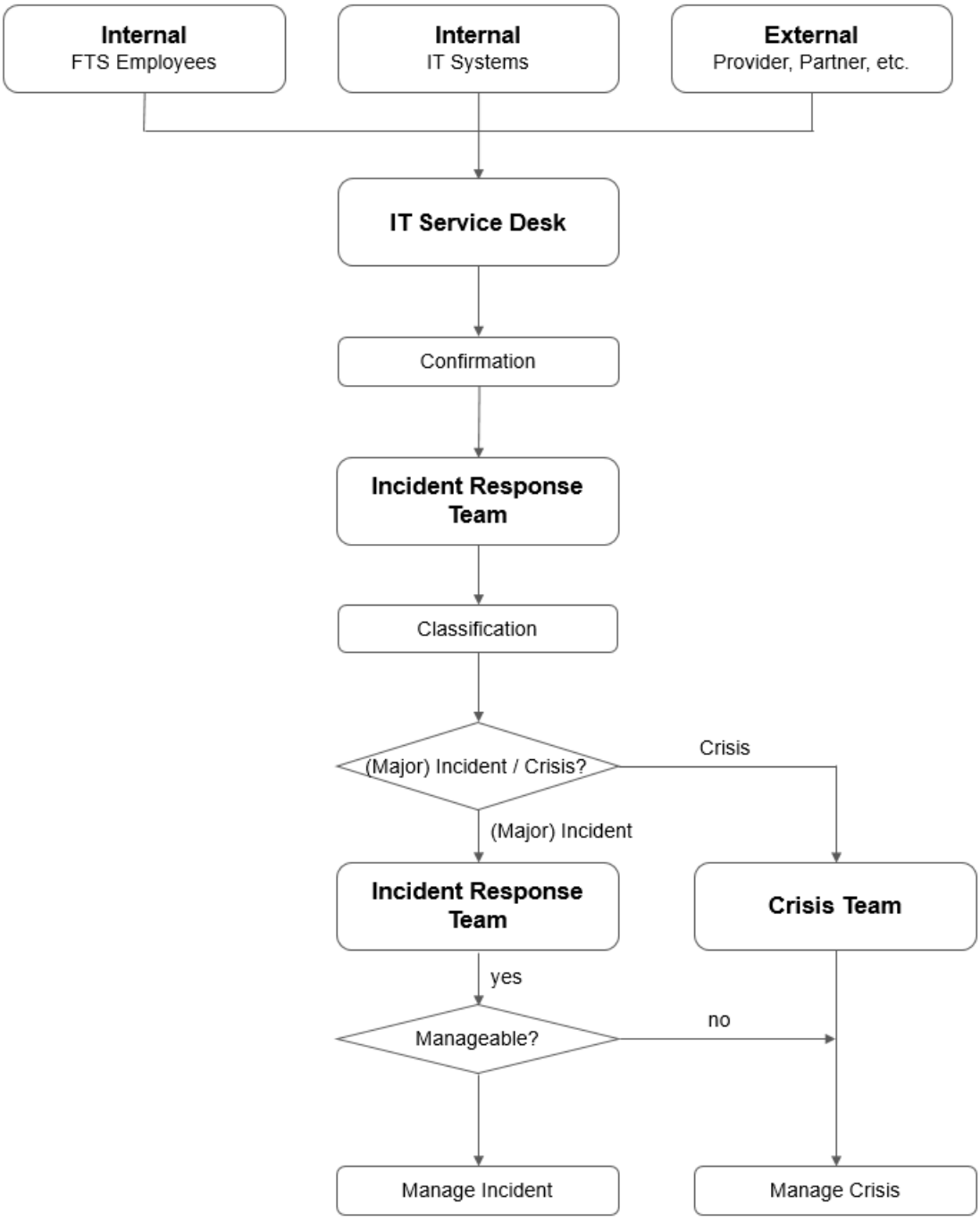

Figure 3: Incident Response Management Process

6 Identification and Confirmation

FTS employees who discover an incident are obliged to report it immediately to the IT Service Desk. The IT Service Desk records the message in the Incident Management Tool, checks and confirms the reported even and informs the incident response manager. The incident logging checklist contains information about the data that must be collected during the incident response management process. FTS employees should be regularly informed about the correct way to report an event.

7 Classification

7.1 Impact

Events are classified according to their impact and urgency. This definition is used both in the ISO/IEC 20000 standard for IT Service Management (ITSM) and in the Information Technology Infrastructure Library (ITIL).

Impact – depends on the number of users/customers affected, financial loss, damage to reputation, etc. and should be assessed on the basis of the information available at the time of detection of the incident

Class	Description
1	Damage with minor, negligible effects
2	Damage with limited and manageable effects
3	Damage with considerable, but not existence-threatening effects
4	Damage with consequences threatening the existence of the company

Table 4: Classification of damage effects

7.2 Urgency

Urgency – results from the time available for emergency response

Class	Description
1	Normal operation within > 24 h
2	Normal operation within 24 h
3	Normal operation within 8 h
4	Normal operation within 4 h

Table 5: Classification of urgency

Alternatively RTO and RPO values could be used for urgency classification.

Class	Description	
1	RTO > 24 h;	RPO ≤ 24 h
2	RTP ≤ 24 h;	RPO ≤ 8 h
3	RTP ≤ 8 h;	RPO ≤ 4 h
4	RTP ≤ 4 h;	RPO ≤ 0 h

Table 6: Classification of urgency

Recovery Time Objective (RTO) - The Recovery Time Objective is the time from the time of the event to the complete recovery of the business processes.

Recovery Point Objective (RPO) - The Recovery Point Objective is the time that may lie between two data backups, i.e. the maximum amount of data/transactions that may be lost between the last backup and the system failure. If no data loss is acceptable, the RPO is 0.

7.3 Event classification

		Impact			
		1	2	3	4
Urgency	1	Incident	Incident	Major Incident	Crisis
	2	Incident	Incident	Major Incident	Crisis
	3	Incident	Major Incident	Major Incident	Crisis
	4	Incident	Major Incident	Crisis	Crisis

Table 7: Classification of incidents

If needed the event classification should be updated during incident response.

7.4 Incident

An incident is a situation in which certain areas, processes or resources do not function as intended, resulting in damage. However, these are not classified as serious. An incident can develop into a major incident and must therefore be closely monitored.

7.5 Major Incident

A major incident is a situation in which essential areas, processes or resources do not function as intended, so that high damage is caused and/or normal operation cannot be guaranteed within the defined restart times. A major incident can develop into a

crisis and must therefore be closely monitored and escalated to crisis management if necessary.

7.6 Crisis

A crisis is characterized by the fact that the existing contingency plans are no longer sufficient to cope with the event. This is particularly true in situations where the existence of the company is threatened. In such a situation the crisis team will be convened. The crisis team coordinates all measures for crisis management and is responsible for overcoming the crisis and returning to normal operations. The crisis management is covered by a separate document.

8 Escalation

If a crisis occurs or a major incident develops into a crisis, the incident response manager immediately escalates to the crisis management team.

- Fides Incident Management Escalation Process
- Appendix 1 Escalation 1.0

9 Containment

Immediate action is taken after an incident has been confirmed. The aim of the immediate measures is to limit the damage.

The checklist for immediate emergency measures contains information on general measures to be taken in all cases and specific immediate measures depending on the incident scenario.

The incident response manager decides on emergency measures. All emergency measures must be documented in the incident management tool.

10 Restart

The aim of restarting is to ensure that business operations can continue in emergency operation with reduced resources and/or an alternative processes.

All steps of the restart process must be documented in the incident management tool.

11 Recovery

The recovery is the transition from emergency operation to normal operation. The restoration of normal operation.

If it becomes apparent that it will take longer to restore normal operation than given by urgency rating, the incident response manager should inform affected users, system administrators, and responsible business management.

All steps of the recovery process must be documented in the incident management tool.

The checklist for recovery measures contains information on general measures to be taken in all cases and specific measures depending on the incident scenario.

As soon as all restart measures have been completed and normal operation is restored, the incident response manager informs affected users, system managers, and responsible business managers. This message also includes any actions that the users must take when restarting the application.

The IT Service Desk updates the status of the incident message on the FTS Intranet and reports the successful restoration of normal operation.

For business-critical systems, it is recommended to create a specific restart plan according a checklist. The system owners are responsible for these restart plans.

The restart plans should be tested by incident response drills.

12 Post-mortem

For incidents that have been classified as crises and for incidents of business-critical systems, a post-mortem analysis must be carried out. The incident response manager can request a post-mortem analysis at any time if this appears to be appropriate.

The incident response manager commissions the system manager to perform the post-mortem analysis. If several systems, infrastructure components or services are affected, the incident response manager decides which unit takes the lead in the post-mortem analysis.

The post-mortem analysis has the following objectives:

- Determine the root cause of the incident
- Document of positive and negative experiences (lessons learned)
- Identify the need for action to continuously improve the operation of IT systems, IT services and IT emergency management
- Propose improvement measures

For the post-mortem analysis and report, the appropriate template should be used.

The post-mortem analysis report must be submitted to the incident response manager within one month after normal operations has been restored.

The incident response manager organizes a post-mortem meeting within two weeks after submission of the post-mortem analysis report to discuss the results of the post-mortem analysis and to agree on any improvement measures.

13 Computer Security Incident Response Team (CSIRT)

The incident response manager decides whether the computer security incident response team (CSIRT) should be called in. The use of the CSIRT is particularly recommended in the event of cyber attacks and in cases of suspected fraud or misconduct.

If investigations are to be carried out where FTS employees are involved (e.g. potential fraud, sexual harassment, mobbing), the use of the CSIRT must be approved in advance by the legal department.