SP3.03.01_003_SOP

manage IT incidents

current version: 2.0

	name	role	approval date	signature
author	herwig albert	IT manager	27 August 2023 | 07:37:02 CEST	DocuSigned by: Herwig Albert B66F4C0C82C247B...
author	joni haeck	program director CxO	28 August 2023 | 09:19:03 CEST	DocuSigned by: Joni Haeck 02365AAD5959444...
revised by	andy stynen	CEO	01 September 2023 | 11:57:34 CEST	DocuSigned by: Andy Stynen 454E2425E54F4E2...
approved by	kimberley walckiers	quality director	01 September 2023 | 14:24:16 CEST	DocuSigned by: Kimberley Walckiers C2DF779B5F094FD...

version and modification control

version	date	reason for modification
2.0	24AUG23	approved version
1.1	07AUG23	update to add a link with new SOP IT change management
1.0	11NOV22	approved version
0.1	24JUN20	initial draft version

table of contents

1 purpose

This document describes the process of analysing, dispatching and handling a detected incident.

The purpose of the incident management process is to restore normal service operation as quickly as possible and minimise the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

2 scope

2.1 in scope

IT infra and CxO

- incidents detected by proactive monitoring
- incident detected by any Ausy collaborator

2.2 out of scope

- change requests
- external supplier request

3 normative references

ISO 9001:2015 quality management systems - Requirements

- § 7.1 Resources
- § 8.1 Operational planning & control

4 related documents

doc id	doc name
SP3.01.02_002_SOP	emergency response plan IT
SP3.01.02_003_SOP	disaster recovery plan IT
SP3.03.03_001_SOP	IT change management

5 definitions and abbreviations

5.2 definitions

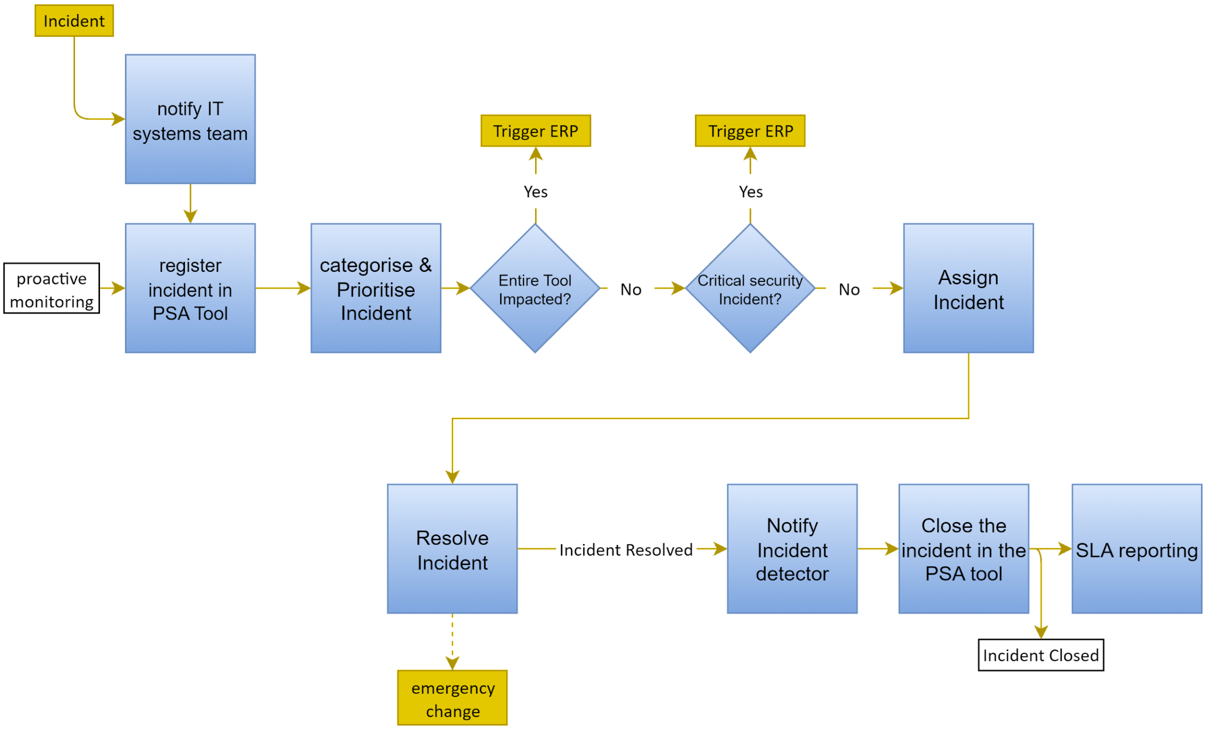
name	definition
Incident	an unplanned interruption to or quality reduction of an IT service (ref.ITILv3)
ITIL	Information Technology Infrastructure Library, a globally recognized collection of best practices for managing information technology (IT)
IT Tool	hardware of software platform used for the daily business operations
PSA Tool	tool used for ticket management, incl. prioritising, categorising, assigning, follow-up and reporting
Ticket	a registered incident or support request within IT.
Critical security incident	A (critical) security incident is an event that may indicate that an organisation's systems or (GDPR) data have been compromised or that measures put in place to protect them have failed.

5.3 abbreviations

abbreviation	definition
Ca	Circa
PSA	Professional Services Automation
ITM	IT Manager
ERP	Emergency Response Plan
SE	System Engineer
SLA	Service Level Agreement
TL	Team Lead Systems Team
PD	Program Director

6 procedure

6.1 process flow



6.2 explanation of the process flow

When an incident occurs the person who detects the incident (incident detector) notifies the IT systems team. This notification can take place by ticket registration, by email, by phone call or by face to face contact. The system engineer registers the incident in the PSA-tool.

As an alternative "incident detector" software is used to detect imminent failures or failures to IT hard- and software, also referred to as "proactive monitoring". These incidents are registered automatically in the PSA-tool.

Upon registration the System Engineer analyses the ticket to determine category and priority of the ticket.

6.2.1 ticket priority

This priority is determined by the combination of urgency and impact of the incident as shown in the below table.

		Impact		
		HIGH	MID	LOW
Urgency	HIGH	1	2	3
	MID	2	3	4
	LOW	3	4	5

6.2.2 ticket category

A ticket category describes in one or maximal 2 levels the subject where the issue is noticed (e.g. "network -> Wifi" or "Google -> Sheets") and is created for reporting purposes only. A non-exhaustive list of suggested categories is available in the PSA tool.

If the incident impacts one or more entire tool(s) for all users, the ERP is triggered (see SOP emergency response plan IT in section 4 related documents) and the regular incident management process ends.
If the incident is categorised as a critical security incident (see definitions in section 5), the ERP (see SOP emergency response plan IT in section 4 related documents) is triggered as well and the regular incident process ends.

If the ERP is not triggered, the ticket is assigned to a system engineer within the IT infra support team or CxO team. He/she becomes responsible for resolving the incident or getting the incident resolved by the supplier.

Once the incident is resolved, the ticket is marked as closed in the PSA tool. If applicable, the incident detector is notified.

6.2.3 SLA reporting

SLA reporting is done on a monthly basis. Following SLA are defined.

service level	high	mid	low
service window	**24 x 7** 365 working days/year Ca. 8760h	**9 x 5** Mo – Fr from 08.30 – 17.30 260 working days/year Ca. 2340 hours	
availability average per year per configuration item	Minimal 99% within service window		
downtime average per year per configuration item	Maximal 1% within service window		
incident reaction time (result obligation)	<= 30 minutes	<= 2 h	<= 8 h
incident resolve time (effort obligation)	<= 1 working day	<= 2 working days	<= 5 working day
continue effort outside the service window?	YES	NO	NO

6.3 responsibilities (RACI)

activity	responsible	accountable	consulted	informed
notify IT	ausy collaborator	ausy collaborator	-	-
register incident	SE	PD (CxO) - TL (Infra)	-	-
categorise & prioritise incident	SE	PD (CxO) - TL (Infra)	ITM	-
resolve incident	SE - Supplier	PD (CxO) - TL (Infra)	-	-
close incident	SE	PD (CxO) - TL (Infra)	ITM	-
notify incident detector	SE	PD (CxO) - TL (Infra)	-	incident detector
SLA reporting	PD (CxO) - TL (Infra)	PD (CxO) - TL (Infra)	-	-

7 annexes

doc id	doc name
-	-