

**Independent investigation of the
major incident occurred on the
15th of June 2022 at skyguide**



1.	Introduction	5
1.1.	Purpose	5
1.2.	Scope	5
1.3.	Structure of this document	6
2.	Method and Structure	7
3.	Fact Finding	9
3.1.	Information Baseline	9
3.2.	Scope and Structure	9
3.3.	Communication	12
3.3.1.	Internal Communication	12
3.3.2.	External Communication	12
3.4.	Major Decisions	13
3.5.	Crisis Organization skyguide (COS)	14
3.6.	Network	23
4.	Conformity Analysis	29
4.1.	Conformity Analysis Summary	30
4.2.	Communication	31
4.2.1.	Internal Communication	31
4.2.2.	External Communication	32
4.3.	Major Decisions	35
4.4.	Crisis Organization skyguide	38
4.5.	Network	42
4.5.1.	Network engineering and operations governance	43
4.5.2.	Network Architecture and monitoring, HA and DR capabilities	47
4.5.3.	13 th of June 2022	49
4.5.4.	14 th of June 2022	52
4.5.5.	15 th of June 2022	53
4.5.6.	Summary of events / conclusion	56
5.	Conclusion	60
5.1.	Overview	61
5.2.	Network	62



5.3.	Crisis Management	75
6.	Recommendation.....	77
6.1.	Prioritization.....	78
6.2.	BCM Governance & Strategy	81
6.3.	Overarching Architecture & Resiliency	85
6.4.	Business Continuity Plans, Processes and Checklists	88
6.5.	Network Operation & Engineering Governance	92
6.6.	Monitoring & Integration	97
7.	Appraisal of internal investigation report	100
7.1.	Communication, Major Decisions, COS	100
7.2.	Network.....	102
8.	Appendix Network Findings.....	104
8.1.	Architecture	104
8.2.	Segmentation	107
8.3.	Product Life Cycle Management	109
8.4.	Security.....	110
8.5.	Continuous Service Improvement.....	112
8.6.	Monitoring.....	117
8.7.	Isolation and Failover Tests	121
8.8.	End-to-end Service Fulfillment	123
8.9.	Employee Training Concept	125
8.10.	Change Management	127
9.	Appendix Crisis Management Findings	129
9.1.	Business Continuity Management	129
9.2.	Disaster Recovery	130
9.3.	Crisis Management	131
9.4.	Detailed background and dedicated questions	133
9.4.1.	Adhering to COS Process	133
9.4.2.	Communication, Collaboration and decision-making process.....	136
9.4.3.	Stakeholder opinions on communication	137
10.	Appendix Information Basis	138
11.	Appendix Timeline.....	148



12.	Appendix Key Definitions	158
13.	Appendix Questions	160
13.1.	Technische Störung	160
13.2.	Krisenmanagement	161
14.	Appendix Abbreviations	162
15.	Appendix Overview Interviews	164



1. Introduction

During the night of 15th June 2022, skyguide experienced a major IT service incident that has caused a "Clear-the-Sky" event. Skyguide has initiated an internal investigation and already provided the report to the Federal Department of the Environment, Transport, Energy and Communications (DETEC). Due to the magnitude of the incident, DETEC commissioned Accenture to conduct an independent investigation.

1.1. Purpose

The objective of this document is to determine the root cause that led to the "Clear-the-Sky" situation on 15th of June 2022, and a subsequent "zero traffic" for five hours. Furthermore, the internal investigations conducted by skyguide since 15th of June 2022 and the crisis management applied should be critically reviewed. Last, preventive and corrective measures and potential improvements should be proposed.

1.2. Scope

To investigate the technical malfunction of 15th of June 2022 at skyguide, events that have occurred will be identified, actual processes for conformity with the expected procedures will be evaluated and conclusions from an independent position will be made. In scope of this investigation are questions related to network devices affected by the incident occurred on the 15th of June 2022 and related crisis management process conformity. Application and server layer are not in scope of this investigation and should be further assessed.

The contents of this investigation should not be considered legal or regulatory advice. Finally, the conclusions drawn from this investigation and their implementation, including with respect to the recommendations made, are the sole responsibility of the relevant recipients of this report.



1.3. Structure of this document

This document is structured in accordance with the book of specification and contains the following chapters:



Figure 1: Overview of Structure and chapters



2. Method and Structure

The investigation is conducted according to Accenture's Business Continuity and Disaster Recovery Framework considering skyguide's specific Safety Management context. Figure 2 shows the mapping of questions to be answered in accordance with the book of specifications (Pflichtenheft). In scope of this investigation are 1) questions related to technical malfunction and 2) questions related to crisis management shown in chapter 13.

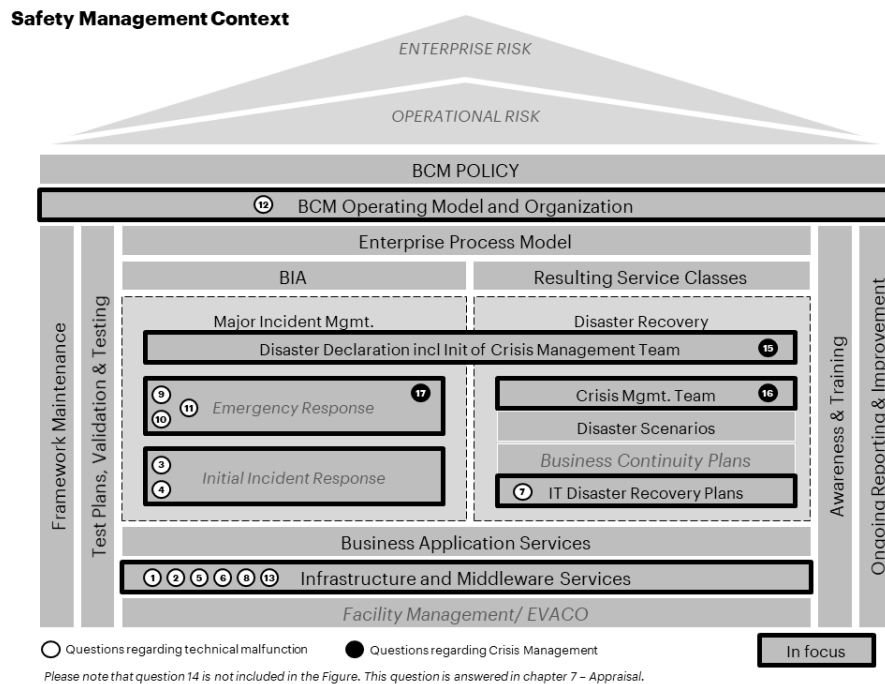


Figure 2: Overview of applied Accenture's Framework and mapping of relevant questions

The investigation is structured into **3 main phases**:

Phase 1: The investigation shows a factual, detailed overview of the process that led to the disruption, when and how the fault was detected and how the fault and its consequences were dealt with. For this purpose, existing material will be screened. Furthermore, a timeline of the crisis including all communication and decisions, and an inventory structure of documentation, will be created.

Phase 2: The key objective of this phase is to complete the fact-finding and compliance analysis phase. For this purpose, structured interviews with key stakeholders will be conducted and relevant business continuity – and crisis management organization, network topology- and monitoring solutions will be investigated. The result is documented in chapter 3 and chapter 4.



Phase 3: During the phase 3, the report is finalized. For this purpose, conclusions and recommendations for collaborations, communication and decision-making will be established. As a result, chapter 5 provides answers for each question listed in the Figure 2. Chapter 6 provides a final recommendation.



3. Fact Finding

The objective of this chapter is to provide a brief overview of what happened as part of the major network incident on the 15th of June 2022. Events are placed (without interpretation) in their factual context:

- Chapter 3.1 provides an overview of information and related documentation requested for this investigation and provided by skyguide (information baseline).
- Chapter 3.2 describes the scope and structure applied for the fact-finding analysis.
- Chapters 3.3-3.6 describe the events related to system, hardware and software. The actions, responses and communications of technical personnel and the decisions, controls and communications of the managers are brought into a comprehensible overview.

3.1. Information Baseline

During the first phase, skyguide's current information basis containing relevant documentation are evaluated. Chapter 10 shows a detailed overview of what information was requested and a mapping to the documents which have been used for this investigation. All dates and times provided in this document are in UTC time zone.

3.2. Scope and Structure

During the first phase of this investigation, information and related documents provided by skyguide have been analyzed. One major finding during this phase was skyguide's internal investigation report contains events related to internal and external communication, major decisions, COS (Crisis Organization skyguide) and Network Operation only to some minimal extent.

Thus, this investigation focuses on the following **four major categories** which are also an integral part of the applied framework shown in Figure 2 outlining the mapping of questions to be answered as part of this investigation:

- 1) **Communication:** Internal and external communication with key stakeholders and appropriate communication plans and related stakeholder communication requirements.
- 2) **Major Decisions:** Gives an overview of major decisions taken by COS-Board or any other relevant function.
- 3) **COS:** Provides an overview of COS-Management related communication and information including COS-Board meetings and related meeting series.
- 4) **Network:** Provides an overview of not only technical events on a switch-log basis, but also events triggered by Level 2 - Network Operations and Level 3 - Network Engineering which have led to the resolution of the problem.



Figure 3 provides an overview of the major events of each category described above. The overview is structured according to skyguide's BCM (Business Continuity Management) Framework and its phases (Response, Recovery, Emergency- and Crisis Management, Recovery Task Force). Please note that this overview contains the main events but does not contain every single phone call and events related to network which already occurred on the 13th of June 2022. A more detailed timeline can be found in chapter 11.

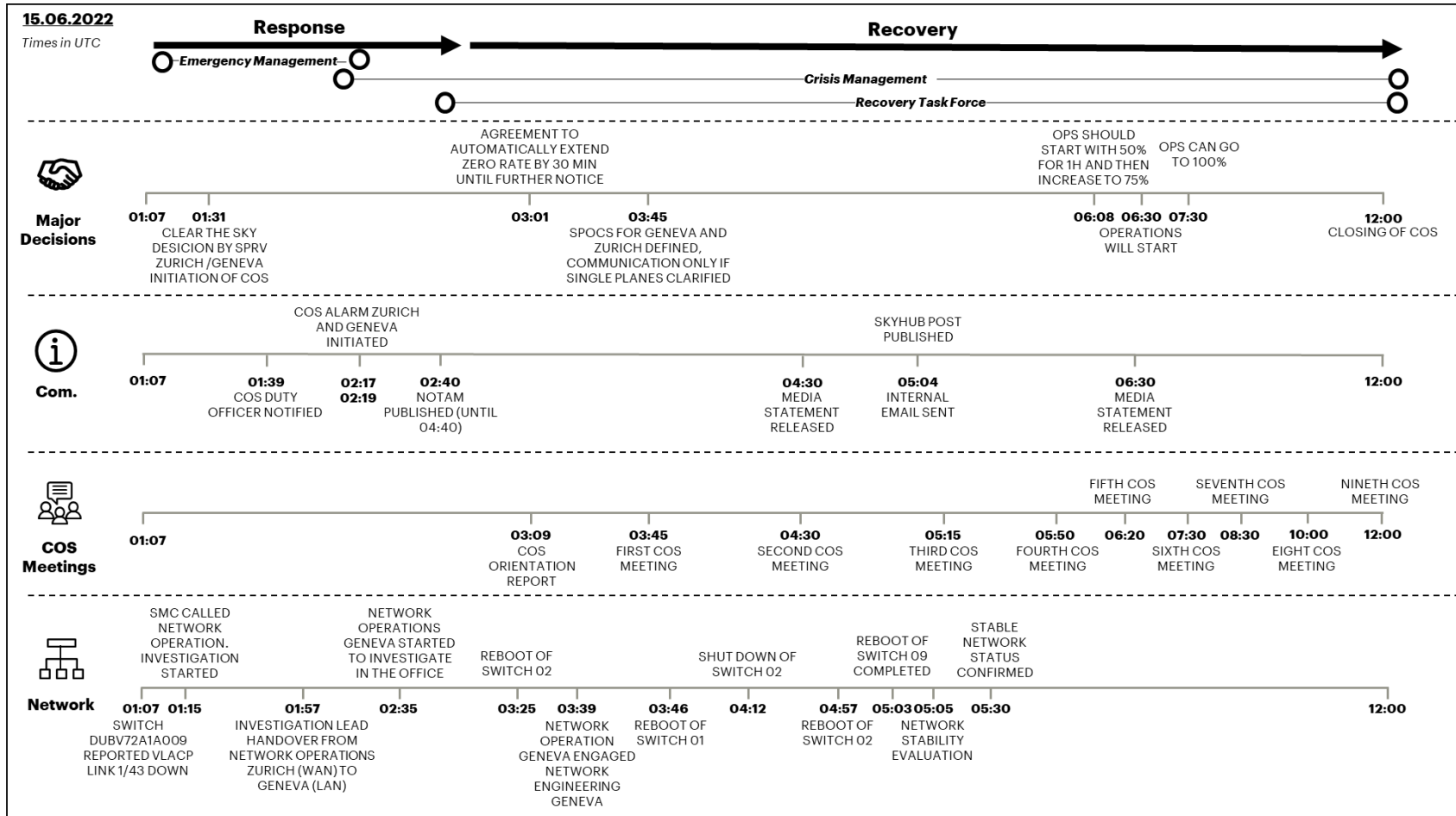


Figure 3: Overview of Timeline



3.3. Communication

This chapter describes internal and external communication provided by skyguide in the event of the 15th of June 2022. To validate the data provided to the investigation team, a one-hour interview with the communication team was conducted.

The crisis communication cell was alerted by the COS mobilization process at 02:17 and 02:19 on 15th of June 2022. The distribution of COS members to Zurich and Geneva was internally aligned. The following setup was put in place:

- Media Spokesperson in Zurich
- Media Spokesperson in Geneva
- Executive in Geneva
- Executive in Zurich
- Head of Communication in Zurich
- Internal Communication in Zurich

3.3.1. Internal Communication

Internal communication to the employees was mainly provided using the intranet (skyhub) but also by email. The first internal update was provided via e-mail at 05:04 to all employees informing the employees that skyguide experienced a technical malfunction which forced the Swiss airspace to be closed until further notice. This was followed by an intranet post using skyhub at 05:05 containing similar information. Both messages contained a reminder not to pass information to external parties. The skyhub post was updated as newer information became available and employees were able to follow the newest developments there. People were able to ask questions using the comment function and some of the comments were responded to by the internal communications team and other COS members. On 17th of June 2022 an update video of the CEO (Chief Executive Officer) was released on skyhub sharing his thoughts on the events on the 15th of June 2022. On 22nd of June 2022 a first internal report on the events of the 15th of June 2022 was shared with the employees on skyhub. In addition, a dedicated intranet page was put together where employees could gather additional information.

3.3.2. External Communication

External communication was provided using media releases, social media platforms and interviews. The first media release was published at 04:30 informing that a technical malfunction had occurred. This media release was reviewed and approved by the head of communication prior to the release. This was followed by a post on Twitter linking to the official media statement at 05:03. The various stakeholders were informed by the CEO and COO (Chief Operating Officer) on a regular basis using E-Mail, Phone, SMS and WhatsApp. Once the issue was resolved another media release was issued at 06:30 informing that the technical malfunction was resolved, and the flight operations could



resume. Throughout the next hours many media requests were served. Skyguide's CEO spoke to the media after the incident and expressed his regret and apologized for the inconveniences.

3.4. Major Decisions

This chapter describes the major decisions taken by the different involved parties on the 15th of June 2022. To complement and validate the major decisions taken during the emergency and crisis management phase, a one-hour interview with the Crisis Manager, Chief of Staff and Business Continuity Manager was conducted.

During a crisis within such a complex ecosystem, various stakeholders must be considered as part of skyguide's crisis management decision process. Figure 4 provides an overview on the most important parties which were involved in the decision making on the 15th of June 2022.

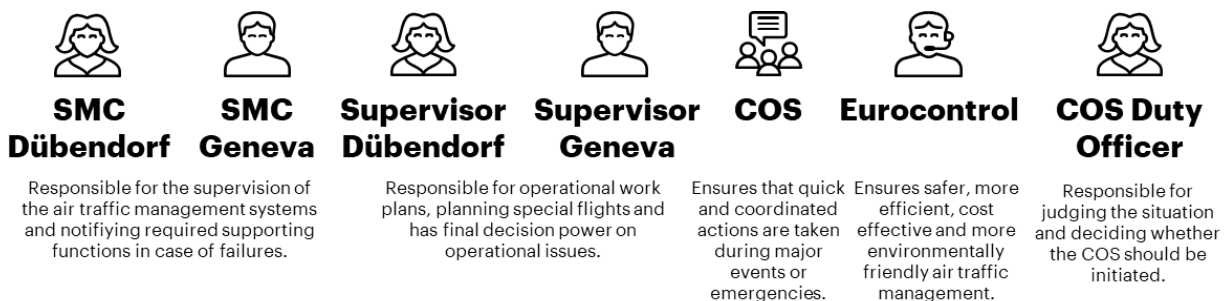


Figure 4: Major Stakeholders for Decision

At 01:07 on 15th of June 2022, a major disruption of skyguide's IT Infrastructure was detected by Systems Monitoring and Control (SMC) Geneva and Zurich resulting in tickets I220615_0001 and I220615_0003. Multiple important applications were impacted by the disruption. The related findings were reported by Level 1 - SMC to the Air Traffic Supervisors. At 01:24, the current situation was discussed between the supervisor ACC in Zurich and the supervisor ACC in Geneva. It was concluded that both ACCs were impacted by similar issues reported by Level 1 - SMC. The supervisors were in constant exchange with the Level 1 - SMC at their respective location. At this point in time (01:31), the Level 1 - SMCs were not able to provide an estimation for the time needed to resolve the issue. Thus, the decision was taken by both supervisors to initiate the "Clear-the-Sky" procedure and to initiate the COS process by notifying the On-call Duty Office. The COS was then mobilized on the decision of the COS Duty Officer Zurich using the COS mobilization process at 02:17 and 02:19 on 15th of June 2022. No further traffic was accepted by the air traffic controllers in Zurich and in Geneva which led to a complete shutdown of the Swiss air traffic (except single planes at the beginning). Not accepting further traffic was retained and constantly prolonged with Eurocontrol by the supervisors and the COS, until



the Level 1 - SMC and technology support teams could provide a resolution estimate or resolution.

It was communicated at 6:08 that resuming of the operations is possible with a capacity of 50% for the first hour, which can be later increased to 75%. In the COS meeting at the 6:20, positive evidence was presented for the resolution of the technical issue. Therefore, it was suggested by the COS that the operations can be resumed. This suggestion was then communicated by the operational COS SPOCs to supervisors. Thus, the supervisors took the decision to resume operations. In the COS meeting at 7:30, it was suggested that the operations could be resumed at full capacity. This was then communicated to the supervisors. This suggestion was applied under the condition that CNS (Communication, Navigation and Surveillance) services won't be affected. The COS has given the possibility to the supervisors to run at a lower rate if required. The BoC (Board of Crisis) was officially closed in the COS meeting at 12:00. To ensure smooth maintenance planned for the upcoming night a task force was defined.

3.5. Crisis Organization skyguide (COS)

To complement and validate the COS-related information taken during the emergency and crisis management phase, a one-hour interview with the Crisis Manager, Chief of Staff and Business Continuity Manager was conducted.

The Crisis Organization skyguide contains three main components: an organizational structure, a defined process, and an alerting tool. Figure 5 represents the COS organization. The alerting tool (e-Alarm emergency tool) is used for mobilization. A text message with a basic description of the issue was sent to pre-inform the predefined contact numbers. A call was then triggered by the alerting tool in order to request COS members to mobilize. The tool can automatically recognize if an individual did not respond. In such a case, the deputy of this individual is contacted automatically.

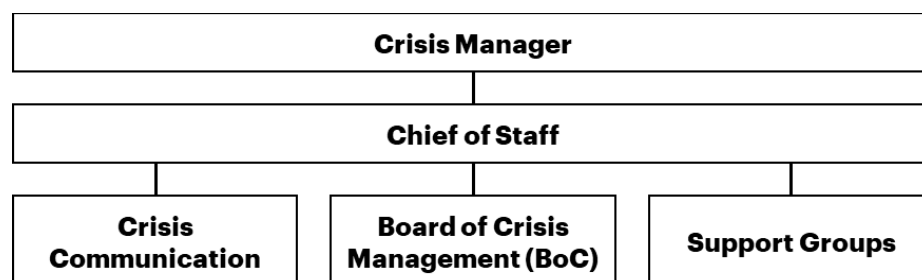


Figure 5: Crisis Management Organization

The mobilization on 15th of June 2022 was initiated by the Duty Officer in Zurich. The mobilization was executed by the COM Center in Geneva at 02:17 for COS HQ Zurich and 02:19 for COS HQ Geneva. As part of the crisis organization, a series of meetings was conducted. Each meeting has a predefined member list, goals and priorities. The following



tables provides a summary of each meeting, including the time, objective, results, and decisions taken.

COS Orientation report	
Time	03:09
Goal	Provide an overview of the situation
Results and Decisions	<p>This meeting was held in Zurich, with the members being already present in the COS room.</p> <ul style="list-style-type: none">• The attendees were informed, that ACC (Area Control Center) Geneva has triggered the COS via Duty Officer Zurich due to a technical malfunction. Eight systems were affected.• Zero rate has been published until 06:00. Problems occurred when publishing NOTAM (Notice to Airmen)
Next Meeting planned	03:45

Table 1: COS Orientation report

First Meeting of BoC (Board of Crisis Management)	
Time	03:45
Goal	Provide common understanding of the situation and regain operational capabilities
Results and Decisions	<ul style="list-style-type: none">• BoC assigned Single Point of Contacts (SPOCs) for operations in Geneva and Zurich and a Crisis Manager• The mission was defined as seeking information, regaining operations and to ensure the situation is stable and safe before increasing capacity• Media release was being prepared• Decision was made that the communication, both internal and external, should only be done when there is clarity about the acceptance of traffic
Next Meeting planned	04:30

Table 2: First meeting of BoC



Second Meeting of BoC	
Time	04:30
Goal	Identify root cause of the problem
Results and Decisions	<ul style="list-style-type: none">• The press release and internal update were being ready for release• Air traffic was still not accepted (rate zero)• Discussion was opened to review if single flights can be accepted• The current understanding of the issue was that an L3 network switch was misbehaving• Partners (Swiss, easyjet and Airport Geneva) were sending representatives to skyguide's premises• The physical safety of passengers was not impacted• No signs of cybercrime activity were detected• The STSB (Swiss Transportation Safety Investigation Board) was already informed• The air force was able to handle flights independently in case of serious emergencies• A discussion about the operational minimal service was raised; definition of COS = Radio, Radar, and CNS• Urgent measures were defined:<ul style="list-style-type: none">○ Extension of the NOTAM○ Assess impact on WTO conference○ Definition of IT minimal service
Next Meeting planned	05:15

Table 3: Second Meeting of BoC



Third Meeting of BoC	
Time	05:15
Goal	Provide situation overview and to manage the crisis
Results and Decisions	<ul style="list-style-type: none">• Swiss Airlines and the Airport Geneva had joined the BoC• The media release had been published and the NOTAM was required to be extended.• VFR (Visual flight rule) operated traffic was reported to not be affected• The root cause was identified on network level and the resolution was ongoing• The situation was rated as bad but under control• It was highlighted not to lose the control of the situation when starting operations again• An update on the WTO conference stated that everything was under control, but delays could happen when flying out of Geneva• At 05:27 the network problem was identified, and systems started to resume connectivity• Systems are starting to update their status as operational in the SMC monitoring overview• It was decided that NOTAM should still be published until 07:00 and could be cancelled earlier if required.
Next Meeting planned	05:50

Table 4: Third meeting of BoC



Fourth Meeting of BoC	
Time	05:50
Goal	Provide an update on the situation
Results and Decisions	<ul style="list-style-type: none">• Flughafen Zürich AG joined the BoC• The systems were recovering• The network team in Zurich was monitoring stability of the network• COS is waiting for the green light of all affected technical system (including applications, servers)• The operations were on standby• Resuming operations was considered only if communication systems were available• The alerting service was working again but flight plans did not reach units like FIC (Flight Information Center) and ACC• The partners were providing a brief update; Flughafen Zürich AG was asking about the rate at the restart and requested prioritization of the inbound traffic
Next Meeting planned	06:20

Table 5: Fourth meeting of BoC



Fifth Meeting of BoC	
Time	06:20
Goal	Provide an update on the situation and define the restart of operations
Results and Decisions	<ul style="list-style-type: none">• Easyjet (GVA) joined the BoC• Media statement was ready to be released once operations would resume• Operations supervisors were clarifying if remaining system errors were critical• CNS services were reported not to be affected by the issue• It was suggested to start with 50% capacity in the first hour and then increase to 75% after that• The partners were providing input on their suggested priorities• At 06:30 it was suggested to resume the operations and to cancel the NOTAM• Retaining documentation was highlighted for investigations of STSB
Next Meeting planned	07:30

Table 6: Fifth Meeting of BoC



Sixth Meeting of BoC	
Time	07:30
Goal	Situation update and how to proceed with resuming the operations
Results and Decisions	<ul style="list-style-type: none">• The information that the airspace is open again was provided to the public• Operations were reported to run at 50% capacity• Additional air traffic controllers were planned for the evening• It was considered that operations could directly increase to 100% capacity• The systems were running again but it was still unclear what caused the outage, and the suppliers were involved• The infrastructure maintenance work was suspended for today• The partners were providing updates from their side• The situation was generally rated as safe and under control• It was highlighted, that caution is required for the AIRAC (Aeronautical Information Regulation and Control) update planned for the next night• Approval of allowing operations at 100%<ul style="list-style-type: none">◦ Supervisors were allowed to run a lower rate given the external circumstances• An IT minimal service concept was still required in case technical problems occur again<ul style="list-style-type: none">◦ Tech and Ops to prepare
Next Meeting planned	08:30 (reduced), 09:30 and 12:00

Table 7: Sixth Meeting of BoC



Seventh Meeting of BoC (reduced)	
Time	08:30
Goal	Situation update and how to proceed with resuming the operations
Results and Decisions	<ul style="list-style-type: none">• The communication department received many interviews requests• Operations were running stable, and a checklist was available in case another degraded mode is required• An IT system overview will be available at 09:30• Technology group was preparing IT minimal service list• The monitoring was increased (duplicated)• IT minimal service list was supposed to be discussed at 10:00
Next Meeting planned	10:00

Table 8: Seventh Meeting of BoC

Eighth Meeting of BoC	
Time	10:00
Goal	Situation update
Results and Decisions	<ul style="list-style-type: none">• Operations were reported to run smoothly, and additional staff was activated for the evening• Investigation on the root cause was still ongoing• Root cause of the problem was discussed. It was pointed out that communication between certain systems did not work. Official communication to FOCA (Federal Office of Civil Aviation) and NTSB had been sent out• Situation was seen as controlled. The crisis board was planned to be closed at 12:00 with a maximum response time of 30 minutes• The group was planned to be on standby until the next day
Next Meeting planned	-

Table 9: Eighth Meeting of BoC



Nineth Meeting of BoC	
Time	12:00
Goal	Situation update
Results and Decisions	<ul style="list-style-type: none">• Skyguide received many additional requests for interviews• The supplier was investigating and trying to identify the root cause• Logs were analyzed to exclude the possibility of a cyber-attack• A task force was set up to decide and ensure the maintenance work the following night were running smoothly• The COS was officially closed• Task force was running independently
Next Meeting planned	Task force meeting to be set up

Table 10: Nineth Meeting of BoC

Task force meeting	
Time	18:00
Goal	Situation overview and decide on the AIRAC release
Results and Decisions	<ul style="list-style-type: none">• Mitigation and preventative measures were in place• It was decided to apply only releases considered to be highly critical
Next Meeting planned	-

Table 11: Task force meeting



3.6. Network

This chapter provides an overview of technical and organizational events related to the 15th of June 2022. In scope of our investigation are switch logs between the 13th – 15th of June 2022.

To validate the information provided to the investigation team, five interviews have been conducted with relevant skyguide's stakeholders:

- A **first session** was conducted to understand skyguide's overarching IT architecture, embedded network architecture and its main guiding principles
- The objective of the **second session** was to comprehend the actions taken by the Level 3 - Network Engineering and Level 2 - Network Operations team to investigate and resolve the issue
- The **third session** was conducted to understand the capabilities in place for monitoring skyguide's IT landscape (application, network, system management and controlling).
- The objective of the **fourth session** was to understand the responsibility of the Level 2 - Network Operations team and its demarcation towards the responsibility of Level 3 - Network Engineering
- The **fifth session** served to understand the responsibility of Level 3 - Network Engineering the way they are expected to support Level 2 - Network Operations for project- and operational matters.

Skyguide's network environment for applications used by the flight control operations consists of two independent and identically configured networks: ANS1 and ANS2. ANS is a production network for Air Navigation Services. Both networks can run independently and are redundant. Applications, which were impacted by the events of 15th of June 2022, operate only on the ANS1 network. The investigation focused on analyzing the impacted ANS1 network. All below diagrams and references were made for ANS1 network.

ANS1 network has been visualized on the below Figure 6: Events which occurred on the 13th and 15th of June 2022. The main components of the ANS1 network are VMware ESX Cluster, which consists of two cluster members. It is used for hosting virtualized applications. The virtualized platform is the new environment of skyguide, where legacy solutions are migrated to. VMware ESX Cluster is connected to the network through a redundant network switch cluster, consisting of switch 09 (DUBV72A1A009) and switch 10 (DUBV72A1A010), located in Dübendorf. This allows applications hosted in the virtualized environment to connect to the network. As illustrated below, switch 09 and switch 10 are connected to another redundant network switch cluster, consisting of



switch 01 (DUBV72A1A001) and switch 02 (DUBV72A1A002). The second network switch cluster is used for connecting legacy systems and clients to the network.

Network switches are operating using specific installed firmware versions. In case of the network switches which are in scope of this investigation, the firmware and related bug fixes are provided by the vendor, Extreme Networks. Skyguide has been evaluating provided firmware (firmware in terms of provided bug fixes and new features) and deciding to begin the implementation process or to remain on the currently installed version. At the time of the incident, the installed firmware version was 7.1.0.0 which was released by the network switch vendor in 2018. The firmware versions 8.0.8 and 8.1.2, which were indicated by the network switch vendor as first versions to address the type of issue which occurred on 13th and 15th of June 2022 at skyguide, were released in February 2020. However, release notes for firmware versions 8.0.8 and 8.1.2 provided by Extreme Networks, have not clearly highlighted this type of issue.

Skyguide's network monitoring landscape consists of two technical tools: XIQ and PRTG. XIQ (ExtremeCloud IQ) is a network monitoring tool provided by the same vendor which provided the network equipment – Extreme Networks. It provides the necessary functionality for end-to-end network management, including automation, configuration, firmware management and analytics. The rules for XIQ alerts are setup and configured by Level 3 - Network Engineering. The Level 3 - Network Engineering team defines monitoring alert rules during internal testing and evaluation process. Level 2 - Network Operations team uses these alerts for daily monitoring and evaluation of the network status.

PRTG is provided by a 3rd party vendor, Paessler. It is used by skyguide on network components to perform trend analysis, utilization checks, bandwidth throughput and check load on CPU and network ports. XIQ and PRTG are hosted on separate systems in separate networks. In order to obtain information, XIQ is hosted on a virtualized server and is connecting through firewalls to reach ANS1 network. At the same time, one of PRTG servers is located within ANS1 networks and is connected through an additional layer 2 switch, directly to switch 01 and switch 02.

Historical data in both monitoring systems are handled differently. XIQ monitoring system is focused on presenting most current and up to date information. Access to historical data is possible, however not all functions are available in this view. This may have negative impact on the time needed by support personnel to obtain, analyze and understand the data. PRTG monitoring tool allows to display a selected period, including historical data, allowing for better understanding of the displayed information and their origin.

Although skyguide has two monitoring systems in place, some information, which was crucial during the investigation performed on 13th and 15th of June 2022, is only available



after connecting directly to the network switch through a console or a web interface. This information includes network port and port queue statistics.

It is worth noting, that information available to Level 1 - SMC and Level 2 - Network Operations can be displayed differently, due to differences in configuration between monitoring tools. Some of the systems are providing monitoring data directly to Level 1 - SMC and XIQ, while others are providing data only to XIQ which is then transmitting the information to Level 1 - SMC. Differences in interpretation of data between XIQ and Level 1 - SMC depend on the monitoring alarm configuration in both systems. Another set of differences is caused by XIQ discovery limitations. XIQ automatically discovers and links for devices produced by Avaya and Extreme Networks. Devices produced by other manufacturers must be added manually and all links between devices also need to be created manually. For such devices XIQ does not provide complete support functionality and introduces certain limitations. This may create differences as manual process does not follow a common standard, allowing for differences in naming convention and if all links will be correctly created and updated over time.

Timeline in this report includes events which occurred on switch 09, 10, 01 and 02. Other network devices which were investigated by the support team and were later found not to be the source of the problem, are not included in this report. Below diagram explains high level topology and highlights which connections were affected by the events which took place on 15th of June 2022. All times are provided in UTC time format.

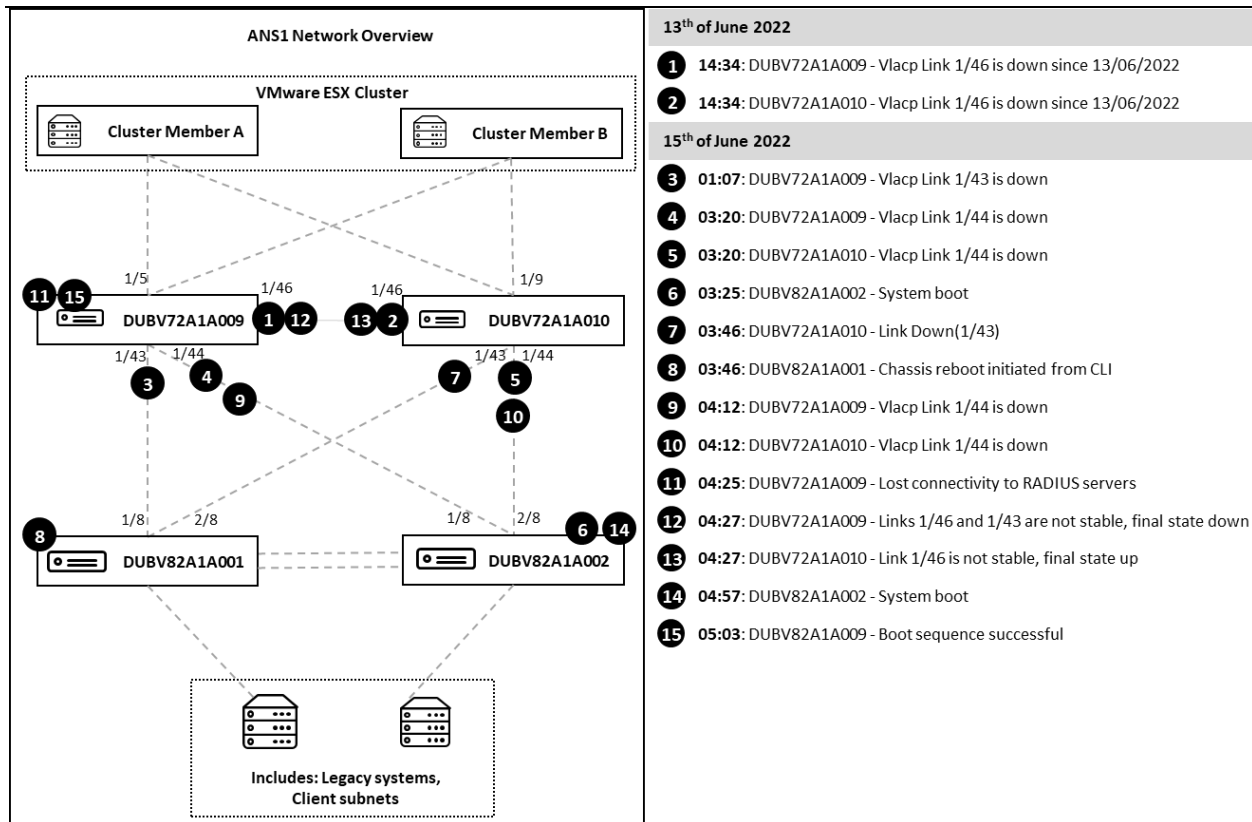


Figure 6: Events which occurred on the 13th and 15th of June 2022

What was found as a precursor of the events which took place on the 15th of June 2022, was an event which occurred 2 days earlier, on 13th of June 2022. All below references are referring to above Figure 6.

On 13th of June 2022 switch 09 malfunctioned. At 14:34, switches 09 and 10 detected that Vlacp Link on port 1/46 is down, however the XIQ monitoring tool was only showing an issue on switch 10. This is shown as (1) and (2) on Figure 6. Switch 10 correctly removed its neighbor switch 09, as the communication was not working (LLDP Neighbor Deleted on interface 1/46). Ports 1/46 are responsible for connecting both switches together. Vlacp is a protocol which allows to check if the data can be sent.

The XIQ monitoring tool was correctly showing the issue reported by switch 10, however it was not showing issue on switch 09. Similarly, incorrect information for switch 09 was also shown on the second monitoring tool, PRTG, while information for switch 10 was correct. When on 13th of June 2022 the investigation took place, there was no disruption to network traffic and all services operated correctly. It is worth noting, that information about holistic network infrastructure is not available at hand to the Level 2 - Network Operations. They are required to check different systems and sources to locate required information. At 15:57, network support connected directly to switch 10 and switch 01 to



investigate the issue. Switch 01 was later accessed again at 16:14. The alert was acknowledged by Level 2 - Network Operations. They evaluated the operational status of the affected port and considered the port as healthy and fully operational. XIQ monitoring tool was checked and affected ports were showing as fully operational. Therefore, it was decided to continue monitoring switch 10 and close the alert afterwards. However, the PRTG monitoring tool was showing that the link between switch 09 to switch 10 was not working correctly as the data transfer stopped. Additionally, PRTG was showing for switch 10 that the port 1/46 connecting to switch 09 had 100% downtime, however it was showing no downtime on the same connection on switch 09.

The network was able to operate without impact on operations through the remaining part of 13th of June 2022 and whole day on 14th of June 2022. This was possible because the communication concluded through switch 01 and switch 02, which acted as an intermediary. However, on 15th of June 2022 new failures occurred.

On 15th of June 2022 at 01:07, switch 09 reported Vlacp link on port 1/43 is down (3), which is a link to switch 01. The network was disrupted, and applications were unable to communicate. At 01:15, Level 1 - SMC called Level 2 - Network Operations, which began to investigate the issue. The monitoring tool still didn't have correct and up to date information about switch 09, which was unknown at the time. XIQ monitoring tool was displaying 9 pages of open alarms, many of which were not investigated and closed when they initially appeared. In the network map overview, only switch 01 was reported as being impacted. If the alert would not have been cleared on 13th of June 2022, switch 10 would also be shown as being impacted.

At 01:45, network support connected for the first time to switch 01 and switch 10 for investigation purposes on this day. Switches 01 and 10 were later again accessed at 02:50. At 02:55 and 03:01 switch 09 was accessed to perform analysis and investigation. During interviews it was confirmed that establishing connection to switch 09 was not possible during initial attempts.

Switch 09 and 10 reported that connectivity to switch 02 is not possible (Vlacp link on port 1/44 is down). This is shown as (4) and (5) on Figure 6. During the interviews, it was confirmed, that PRTG monitoring tool has reported unusual behavior on this port, with data being received by switch 09, however no data was sent. Switch 02 completed system boot after restart at 03:25 (6). Switch 9 and 10 correctly updated their LLDP neighbors during the restart.

Switch 01 was accessed at 03:45 and restarted shortly after (8). Switch 10 correctly detected Link Down (1/43) at 03:46. This is shown as (7) on Figure 6. Switch 09 has not detected any change as it was reporting link down since 01:07. Switch 02 was accessed successfully for the first time at 03:46.



As the network issue was not resolved, switch 02 was accessed at 04:02 and later shut down at 04:12 (9) (10). Switch 01 was accessed at 04:19, 04:23 and at 04:25. At 04:25, switch 09 lost connectivity to RADIUS servers (11), which indicates connectivity issues. At 04:27 network team started working on switch 09 and switch 10 in order to restore connectivity on ports 1/43 and 1/46 (12) (13). Switch 02 was rebooted at 04:57 (14). After logging in directly to Switch 09 and analyzing the data, the team understood what information was missing in the monitoring, verified it on other devices and decided to restart Switch 09. Log information from switch 09 had to be obtained by physically connecting to the switch, as the network connectivity to the switch was not allowing to effectively download the information. Switch 09 completed the booting process at 05:03 and afterwards stability of the network was evaluated. Level 3 - Network Engineering confirmed the status of the network as stable at 05:30.



4. Conformity Analysis

In this chapter the actual events and handling of the situation is compared against the functional requirements, the procedures of the COS and the responsibilities of skyguide. The following table shows the structure of this chapter and the mapping to the questions to be answered as part of this investigation in accordance with the book of specification (see Appendix Questions).

Chapter	Title	Mapped to DETEC question
BCM related topics		
4.2	Internal and external communications	15,16,17
4.3	Major Decisions	15,16,17
4.4	Crisis Organization skyguide	15,16,17
Network		
4.5.1	Network engineering and operations governance	5, 12
4.5.2	Architecture and overarching monitoring architecture, High-Availability and Disaster Recovery capabilities	3, 6, 7, 8, 9, 10, 11, 12
4.5.3	13 th of June 2022	2, 3, 4, 9, 12, 13
4.5.4	14 th of June 2022	2, 3, 4, 9, 12, 13
4.5.5	15 th of June 2022	2, 3, 4, 9, 12, 13
4.5.6	Summary of events / conclusion	1, 5, 12

Table 12: Overview & structure conformity analysis

Please note that question 14 is not included in the table above. This question asks for confirmation of skyguide's internal investigation report which is subject of chapter 7.



The questions listed in the table above are addressed in the following chapters. The conformity is being rated according to the following table:

Rating	Definition of Rating
Fully Conform	Fulfill all requirements applicable for a certain area.
Partially Conform	Fulfill some of the requirements applicable for a certain area.
Not Conform	Does not fulfill any specific requirements applicable for a certain area.
Not Applicable	There are no requirements available to test conformity against. Or topic relies solely on subjective interpretation.

Table 13: Overview and Definition

4.1. Conformity Analysis Summary

This chapter provides a brief overview of the conformity analysis.

Area	Sub-Area	Rating
BCM Communication	Internal Communication – Processes	Fully Conform
BCM Communication	Internal Communication – Stakeholders	Partially Conform
BCM Communication	External Communication – Processes	Fully Conform
BCM Communication	External Communication – Stakeholders	Fully Conform
BCM – Major Decisions	Process – Clear-the-Sky	Fully Conform
BCM – Major Decisions	Process – Resume Operations	Fully Conform
BCM – COS	Organization & Responsibility Mobilization	Partially Conform
BCM – COS	Process effectiveness	Partially Conform
BCM – COS	Collaboration, Communication, Decision-Making	Fully Conform
Network	Network Engineering & Operation Governance	Partially Conform
Network	Network Architecture & Monitoring	Not Applicable
Network	13 th of June – Event Acknowledgement	Fully Conform
Network	13 th of June – Event investigation	Not Applicable
Network	13 th of June – Event resolution	Not Applicable
Network	14 th of June – Event investigation	Not Applicable
Network	15 th of June – Event Acknowledgement	Fully Conform



Network	15 th of June – Event investigation	Not Applicable
Network	15 th of June – Event resolution	Not Applicable

Table 14: Conformity Analysis Summary

The following chapters show a detailed conformity analysis of skyguide's communication, major decisions, COS, and network.

4.2. Communication

This objective of this chapter is to evaluate the conformity of the internal- and external communication provided by skyguide.

4.2.1. Internal Communication

Was the process executed according to skyguide's guidelines?	
Recap applicable Findings	<p>As explained in chapter 3.3, the crisis communication cell was mobilized on 15th of June 2022 at 02:17 and 02:19. Out of five people in the communication cell, two positive responses including an estimated arrival time, two unavailabilities and one no-response were reported. An internal alignment on location assignment was conducted and additional people were mobilized and distributed as described in chapter 3.3.</p> <p>Checklist and template were available for the people if required. The process was known to the individuals as stated in an interview. The internal communication was executed as described in chapter 3.3. Regular updates were provided on skyhub. Comments on the skyhub publications were responded by the internal communications responsible but also by the COO. Further updates were released after the day of the incident on skyhub as well.</p>
How it was supposed to be handled	<p>As per skyguide's COS governance, one person per skyguide's crisis unit functions described in chapter 3.5 shall be mobilized. Role assignments should be executed based on the available individuals. Regular "Crisis Com Meetings" or conference calls to align shall be conducted. Furthermore, the internal communication shall consist out of the following phases:</p> <ol style="list-style-type: none">1. Situation analysis2. Internal pre-orientation3. Ongoing internal information4. Follow-up information + discussion5. Feedback
Interpretation	<p>The mobilization was conducted in accordance with the process mentioned above as the presence of one person is required at the beginning. Skyhub and email was used as a main communication means throughout the process steps one to five. Based on the</p>



	interview internal alignments were conducted. All the major phases were executed in accordance with skyguide's internal communication manual.
Conformity Level	Fully Conform

Table 15: Internal Communication Process Analysis

In the internal stakeholder own opinion, have they been sufficiently informed?	
Recap applicable Findings	As mentioned in Table 15, comments on the skyhub publications were responded to by the internal communications responsible but also by the COO. In addition, the debriefing sessions within the communication team were conducted as reported in an interview. In addition, a high-level qualitative and quantitative analysis was conducted by skyguide for internal communication after the event.
How it was supposed to be handled	Internal stakeholders shall be informed.
Interpretation	<p>The interest within skyguide on the technical malfunctions was relatively high in comparison to other posts. The result of skyguide's internal analysis shows that the internal communication was perceived as effective by its main stakeholders. Feedback of some employees was indicating that information should have been provided more detailed and more frequent. Skyguide has provided direct feedback on these comments and gave reasoning.</p> <p>Our interviews have shown that certain individuals (reception desk & Air traffic controllers (ATCOs)) or groups could have been informed on a more frequent basis. When the operations were resumed, no information/update on the root cause of the technical malfunction was provided to the ATCOs.</p>
Conformity Level	Partially Conform

Table 16: Internal Communication Perception

4.2.2. External Communication

To evaluate how the communication was perceived by skyguide's external stakeholders, an interview was conducted with several key stakeholders as listed in Table 17. The interviewed stakeholders were selected from skyguide's external stakeholder analysis. The following table shows the interviewed stakeholders:



Stakeholder Group	Stakeholder
Government	DETEC
	Federal Office of Civil Aviation (FOCA)
Customer	Swiss International Airlines
Partners	Airport Zurich
	Airport Geneva

Table 17: Interviewed external stakeholders

In addition, an interview with the Chairman of the Board of skyguide was conducted as he received feedback from various external parties on the incident.

Was the process executed according to skyguide's guidelines?	
Recap applicable Findings	<p>As explained in chapter 3.3, the crisis communication cell was mobilized on 15th of June 2022 at 02:17 and 02:19. Out of five people, two positive responses including an estimated arrival time, two negative responses and one no-response was registered. An internal alignment on location assignment was conducted and additional people were mobilized and distributed as described in chapter 3.3.</p> <p>The process was executed as described in chapter 3.3. The first media release was reported to be in preparation in the COS meeting at 03:45. Templates and checklists were available for the team and could be consulted if required. The process was known to the individuals as stated in an interview. The templates were considered as helpful to prepare the contents of the media release in a more efficient way. The first media statement was reviewed and approved by the head of communication part of BoC. The media statements were released as described in chapter 3.3. A mix between Meltwater platform and emails was used for the releases. In an interview, it was stated, that reports of an "Cyber Security Incident" had come up in the media and this was identified and addressed by the external communication team. Media- and interview requests were responded to throughout the day.</p>
How it was supposed to be handled	<p>As per skyguide's COS governance, one person per skyguide's crisis unit functions described in chapter 3.5 shall be mobilized. Role assignments should be executed based on the available individuals. Regular "Crisis Com Meetings" or conference calls to align shall be conducted. The external communication shall consist out of the following phases:</p> <ol style="list-style-type: none">1. Situation analysis2. Content3. External Information4. Mail to all Media



	5. Internet/Intranet 6. Save 7. Ongoing external information 8. Evaluation 9. Follow-up information + discussion
Interpretation	<p>The mobilization was conducted in accordance with the process mentioned above as the presence of one person is required at the beginning. Role assignment and location assignment were conducted. The defined tools were used. Based on the interview internal alignments were conducted. Minor issues were experienced during the media release publication using the Meltwater platform in phases one through four mentioned above. An evaluation was executed throughout the day, and correcting measures were taken as required. Ongoing external information during the crisis was not required due to the duration of the issue. Follow-ups and interviews were provided throughout the day.</p>
Conformity Level	Fully Conform

Table 18: Conformity Analysis - External Communication

In the external stakeholder own opinion, have they been sufficiently informed?	
Recap applicable Findings	<p>Debriefing sessions including major stakeholders were executed as reported in an interview. Regular touchpoints with external partners are planned and were conducted as reported in an interview. In addition, a qualitative and quantitative analysis was conducted by skyguide for external communication after the event.</p> <p>During the crisis Swiss, EasyJet, Airport Zurich, and Airport Geneva were directly integrated into the crisis organization.</p>
How it was supposed to be handled	External stakeholders shall be informed.
Interpretation	<p>Our interviews have shown that external communication was perceived well and suitable by the external stakeholders. Especially highlighted were the short and easy communication paths and availability of the skyguide responsible. The direct integration of external parties into the COS was highlighted as being efficient for information flows by multiple stakeholders.</p> <p>Desired information was reported to be available at the right time for the most interviewed stakeholders.</p> <p>Although there was generally relatively high satisfaction about the communication certain improvements were identified.</p>



	<p>In an interview FOCA was expressing their desire to become member of skyguide's crisis management for future crisis.</p> <p>In an interview DETEC GS was expressing the desire to be informed directly in case of a major disruption of Swiss air traffic. It was also stated, that the DDPS GS was not directly informed about the situation either.</p>
Conformity Level	Fully Conform

Table 19: Conformity Analysis - Perception of Communication

4.3. Major Decisions

This chapter shows the conformity analysis related to major decisions taken.

Was the process that led to the "Clear-the-Sky" decision executed according to skyguide's guidelines?	
Recap applicable Findings	<p>As described in chapter 3.4, the decision to Clear-the-Sky was taken because the Level 1 - SMCs were unable to provide a clear resolution estimate of the technical issue. It was decided by the supervisor ACC Geneva and ACC Zurich to take the same action for both locations at 01:24. The emergency manual was consulted by the supervisor ACC Zurich and by the supervisor ACC Geneva. The failure of multiple systems at the same time was not covered by a scenario listed in emergency manuals. According to the emergency manual, a single scenario concerning a system failure could already require the supervisor ACC Zurich to initiate the Clear-the-Sky procedure, depending on the time specified for a scenario for which a system is not available. Skyguide's emergency checklist applicable for ACC Geneva contains the option of applying a FLAS (Flight Allocation Scheme) or "No traffic mode" in case of emergencies. The emergency case consulted by the supervisor listed both options but stated that "No traffic mode" should be implemented in case both ACCs are affected. As it was previously agreed by both supervisors to implement the same procedure, it was decided to implement Clear-the-Sky/"No traffic mode" at both of the locations. As described in chapter 3.4, it was mutually decided by the supervisors to Clear-the-Sky at 01:31.</p>
How it was supposed to be handled	<p>If a system disturbance is detected the Level 1 - SMC shall stabilize the situation as a first step. The problem shall then be diagnosed by the Level 1 - SMC as a second step. In case of a system disturbance, the Level 1 - SMC and supervisor shall collaborate closely as the Level 1 - SMC shall provide fundamental information to the supervisor. As a next step, remaining systems shall be evaluated. Depending on if vital (would not allow to execute safe air traffic management (ATM)) or essential (reduction of rate or adverse</p>



	conditions for ATCOs) functionalities are missing, a decision should be taken. If vital information is missing, the operations should be suspended which results in the execution of the Clear-the-Sky procedure. If essential information would be missing, a degraded mode would be implemented. Supervisors shall take actions according to their emergency manuals.
Interpretation	<p>Events reported to Level 1 - SMC by various systems were evaluated on its impact and its resolution time. The duration and the lack of resolution estimate were the trigger for the decision to close the Swiss airspace. Given the fact that, scenarios in the emergency manual ACC Zurich already states to Clear-the-Sky if one system fails for a certain time, the supervisors were acting with safety in mind and in accordance with skyguide's procedures. The technical malfunction on 15th of June 2022 impacted multiple supporting systems for ATM. Conducted interviews showed, that essential information like radio, radar and altitude of planes were always available and confirmed by the Level 1 - SMC.</p> <p>The emergency checklists do not contain a scenario where a failure of multiple systems occurs at the same time. In this case, a certain scenario from the emergency checklist could not be applied one-to-one. It must be noted that several scenarios are listed in the emergency checklist applicable for ACC Zurich. According to these scenarios listed in the emergency checklist, a Clear-the-Sky procedure must be initiated by the supervisor depending on the time a single system is not available. Thus, the precaution for a single system failure as listed in the emergency checklist was applied by the supervisor for the situation as of the 15th of June 2022 where multiple systems failed.</p>
Conformity Level	Fully Conform

Table 20: Conformity Analysis - Major Decisions - Clear-the-Sky

Was the process that led to the restart of operations according to skyguide's guidelines?	
Recap applicable Findings	At 05:03, the reboot of switch 09 was completed which led to the resolution of the issue. At 05:05, the network stability analysis was initiated. As described in chapter 3.4; once systems were reported as fully operational to COS, the COS suggested at 06:30 that operations can be resumed by applying a restart rate of 50% for the first hour and then increasing the rate by 25%. This information was communicated to the supervisors and operations were restarting at 50% by the supervisors. The procedure on the emergency manual was executed as reported in an interview by both supervisors.



	<p>Some of the actions were not required to be executed by the supervisor as the SPOC COS was executing those actions. Clearance to run operations at normal level was given in the COS meeting at 07:30 under the condition that CNS is not affected. The supervisors were allowed to run operation at a lower rate if required. In the COS meeting at 08:30, it was reported that increased monitoring was put in place by applying a four-eye principle.</p>
How it was supposed to be handled	<p>Once the solution of the problem is identified, alignment with the supervision team and the operations shall happen for the implementation of the fix. During the recovery of the technical functions, the ATCOs shall conduct fundamental tests by using the respective system. The system shall then be closely monitored in a recovery stabilization phase. Only if all vital and essential functions are available the operations supervisor shall decide to revert to normal mode.</p>
Interpretation	<p>The process was adhered to as intended. All major steps were conducted, the systems were monitored for stability before going live, it was confirmed that vital and essential functions are back and running before resuming operations on a reduced level.</p> <p>In an interview, it was mentioned that it is common practice to start with a reduced rate which would also be applied during major system updates as the checklist do not contain a specific reduced rate guideline. This indicates that general practice was applied for the restart of the operations.</p> <p>In interviews with various people who were part of the COS, it was reported, that the COS does not take the final decision about the restart of operations. The final decision shall be with the supervisor. The interviews showed that COS SPOC provided the supervisors with the information that the technical issue was resolved, and that operation can be resumed. Based on this information, system status and considering applicable checklists, the supervisor took the decision to resume operation.</p>
Conformity Level	Fully Conform

Table 21: Conformity Analysis - Major Decision - Restart operation



4.4. Crisis Organization skyguide

This chapter shows the conformity analysis for skyguide's crisis organization governance.

Was the crisis organization skyguide and its responsibilities put in place according to skyguides guidelines?	
Recap applicable Findings	As described in chapter 3.4, the decision to call the COS was taken by both ACC supervisors on duty during the 15 th of June 2022. The COM Center was instructed by supervisor ACC Geneva to call the COS Duty Officer. The COS Duty Officer Geneva was unavailable, and the COS Duty Officer Zurich had to be contacted. An overview of the situation in Geneva was then gained by the COS Duty Officer Zurich to judge if escalation was required. During the information gathering, an issue with a system in Zurich was reported by AIM to the Duty Officer Zurich. With this additional knowledge the COS Duty Officer Zurich was realizing that it was a companywide issue. As explained in chapter 3.5, the COS was mobilized at 15 th of June 2022 at 02:17 and 02:19. After the mobilization the Duty Officer, Zurich was briefing certain individuals on the situation. The COS Orientation rapport was held at 03:09 with participants in Zurich. Thirteen people were participating at the first COS meeting.
How it was supposed to be handled	The COS process can be initiated by any skyguide employee by notifying the on-call Duty Office about an event by phone. The on-call Duty Office shall then pass the information to the COS Duty Officer. The COS Duty Officer shall be available for such escalations and shall request additional information about the situation. Once an overview is gained, the COS Duty Officer shall decide whether to mobilize the COS or not. The mobilization tool (e-Alert mobilization) shall be used to notify the COS members. The notified individuals shall accept or decline the mobilization and provide an arrival estimate.
Interpretation	The mobilization process was following skyguide's defined process with minor issues. During the escalation, the Duty Officer Geneva was unreachable. This was not blocking the escalation path as there is the same position available in Zurich. There was a communication mismatch between the supervisor ACC Geneva and the COS Duty Officer Zurich regarding the scope of the issue. During the phone call between ACC Geneva and the COS Duty Officer, it was not reported that the issue had a companywide impact. This information was only provided later by AIM to COS Duty Officer. The first meeting (Orientation report) was only held in Zurich and the colleagues in Geneva that had already arrived in the office were not included.
Conformity Level	Partially Conform



Table 22: Conformity Analysis - Crisis Organization skyguide - Initialization

Have the processes within skyguide organizational structures and responsibilities been adhered to?	
Recap applicable Findings	<p>Crisis Organization skyguide</p> <p>Once the COS was initiated, various tasks such as communication, crisis management, and various meetings to align on the situation and define further actions were held. More details on those can be found in chapter 3.5.</p> <p>Operational Processes:</p> <p>Once it was decided to Clear-the-Sky, the procedure was applied by both supervisors. The supervisor ACC Geneva did not have clear instructions available in the emergency manual Geneva on how to implement “No traffic mode”. It was known to the supervisor that it would be required to inform Eurocontrol and the adjacent centers about not accepting any traffic. At 01:34, Eurocontrol was informed by the supervisor ACC Geneva and the rate was set to zero. The same action was taken by the supervisor ACC Zurich at 01:39. The necessary groups were informed by the supervisor ACC Zurich by executing the steps on the emergency checklist.</p> <p>As explained in Table 22, the initialization of COS was also executed by the supervisor ACC Geneva. It was also required to publish NOTAM (Notice to air men) to inform pilots in preparation of their flight to change their route. The AIM (Aeronautical Information Management) in Zurich was called by the COM Center in Geneva to align on the NOTAM content. An email to the NOTAM Office was then sent with the text that should be included in the NOTAM. The NOTAM was then prepared and then sent to Austrocontrol for publication. With the resolution of the technical issue, normal AIM operation was resumed. While the technical malfunction was investigated, certain planes were still required to pass the Swiss airspace (especially at the beginning). The ACC Zurich was accepting single planes while the zero rate was applied, this was not the case for the ACC Geneva. This misalignment was corrected after a short connect between the two supervisors. During the crisis there was certain unclarity of IT minimal service within the organization (see chapter 3.5). As part of the COS, a minimal IT service list was planned to be created.</p>
How it was supposed to be handled	<p>Crisis Organization skyguide</p> <p>Once the COS is mobilized, the COS shall perform crisis management, manage, and implement required follow-up actions. Any mobilization of the COS shall be concluded with a final report about the issue.</p>



	<p>Operational Process</p> <p>The ACC Zurich shall execute the Clear-the-Sky action if a system is unavailable for the time specified for a certain scenario in the emergency manual ACC Zurich. The supervisor ACC Geneva shall implement a FLAS or “No traffic mode” in case of a network failure. The supervisor ACC Zurich shall instruct the sectors to Clear-the-Sky, inform the supervisor tower to stop departures in Zurich, set the acceptance rate to zero, and inform various parties about the situation. A party that shall be informed is the AIM to release a NOTAM with the wording “Swiss airspace is closed due to...”. NOTAMs shall be published by the AIM. In case of system disruption of AIM, Austrocontrol shall publish the NOTAM for AIM. During the implementation of a zero rate, no planes shall be accepted.</p>
Interpretation	<p>Crisis Organization skyguide</p> <p>The COS has executed its tasks as intended. The final report was not yet closed as improvements are still in progress. A collection of lessons learned was put together and the report is planned to be closed.</p> <p>Operational Process</p> <p>Generally, the required actions for implementing a Clear-the-Sky procedure were executed. The ACC Geneva emergency manual intends to incorporate a Flight Level Allocation Scheme (FLAS) or “No traffic mode” in case of network failures. The emergency manual states, that “No traffic mode” should be implemented if both ACCs are affected. For ACC Geneva, there was no Clear-the-Sky action available in the emergency manual. Additionally, there was no guidance available on how to implement “No traffic mode” in the emergency manual ACC Geneva. FLAS was not implemented because the supervisors agreed to take the same actions as both ACCs were impacted.</p> <p>Due to the system failure, the AIM was unable to publish NOTAMs as the application (SCONE) was affected by the system malfunction. A standard contingency plan was applied as documented, the neighboring operation center was contacted (Austrocontrol).</p> <p>The acceptance of traffic during a zero rate is not intended. During an interview it was explained that the situation was under control, as required ATM information was available. In addition, accepting single planes was considered safer than rerouting all plans due to potential safety implication. Throughout crisis, there was certain unclarity about the term of IT minimal service. To address this, an overview of affected IT systems including relevant ANS applications and underlying services (e.g. CNS) was created and</p>



	presented to COS (see reference business capabilities and data flows.pptx).
Conformity Level	Partially Conform

Table 23: Conformity Analysis - Crisis Organization skyguide – Process Operations

What was the collaboration, communication and decision-making process like within the COS team?	
Recap applicable Findings	<p>From our interviews with various people who have participated in the COS, the following information could be gathered:</p> <p>The COS meetings were following a clear structure/agenda as predefined. This was also indicated by the meeting minutes documented by the COS. The dedicated crisis tool (ECMT) was used to document tasks and meeting minutes. The updates during the beginning of the meetings were reported as short (“two sentences”). Individuals, who were not required anymore, were requested to leave the BoC to ensure efficiency and relevancy.</p> <p>Communication was mostly performed within the dedicated teams and then brought into the COS meetings as a result. Required information was collected by COS by contacting the respective representative (e.g. Communication, Technology, Operations). Communication paths were reported to be short. A SPOC for operations in Geneva and Zurich was defined who would connect to the Common IFR Room (CIR). The situation in the Common IFR Room was described as calm and organized. According to the supervisor ACC Zurich there was no hectic in the room.</p> <p>The decision-making process was reported as fact based. Only if valid proof of information was presented to the COS, a decision was taken. This principle was applied for the restart of operations. In addition, some of the COS members did highlight, that the final decisions, like restarts, will always lay with the supervisor on duty at that time.</p>
How it was supposed to be handled	<p>The COS meetings shall be structured according to a predefined agenda. The COS members shall be clearly defined and shall be increased or decreased if required. Each person shall have their role assigned and only relevant people should be present. The crisis tool (ECMT) shall be used to manage and document information centrally. A checklist is available for the chief of staff. Communication and related actions shall be performed within the different follow up task forces and outcomes shall be shared in the COS meetings, if required. No specific requirements are set for decision making within the COS.</p>



Interpretation	<p>The structure of the meetings was applied as intended. The structure seemed to have helped to make collaboration efficient within the COS. The communication within the groups was performed as intended. The decision-making process applied was having safety in mind and was not taking unnecessary risks. Stakeholder groups “Partners” and “Customers” (Table 17) were directly included into the COS, the information could be provided in an efficient way according to the perception of stakeholders.</p> <p>In interviews, it was reported, that the COS process is trained repeatedly which had a positive impact on organized and professional handling of the situation.</p>
Conformity Level	Fully Conform

Table 24: Conformity Analysis - Crisis Organization skyguide - Communication & Collaboration

4.5. Network

The objective of this chapter is to evaluate conformity for the events and tasks conducted in network engineering and operation. The key topics addressed in this section are the comparison of the actual events with what should have happen according to functional requirements related to the Network Support.

The topics are focused on four sections which are analyzing the events from 13th, 14th, and 15th of June 2022. Each of the following section is analyzed from a holistic perspective:

- Network Operation & Engineering Governance and related processes
- Time needed to acknowledge the issue
- Actions taken to troubleshoot the technical problem
- Time needed to identify the root cause and resolve it



4.5.1. Network engineering and operations governance

This chapter describes the conformity analysis of network operation and engineering in terms of governance including skyguide's firmware management governance and network operating manual.

In general, is a well governed firmware management process in place?	
Recap applicable Findings	<p>Our analysis in chapter 3.6 showed the firmware installed on the affected network switches was running on version 7.1.0.0. This firmware version was evaluated and implemented by skyguide in 2018.</p> <p>In October 2021, skyguide has begun testing firmware version 8.4.2. Firmware 8.4.2 could not be implemented due to critical bugs detected during skyguide's testing phase. The decision was made to postpone upgrades until version 8.5.1 would be available. During QBR (Quarterly Business Review) in February 2022, firmware version 8.4.3.0 was recommended by the network switch vendor as minimum maintenance service release level, the release level officially recommended by Extreme Network for bug fix support. The firmware version 8.5.1 was released in April 2022 and by this time skyguide started its evaluation.</p> <p>After the incident on 15th of June 2022, Extreme Networks has recommended to apply firmware version 8.5.1 in their Root Cause Analysis document on 23rd of June 2022. This version is being implemented by skyguide at the time of writing this report. As part of this version release, skyguide has shortened the firmware testing period which was used during 7.1.0.0 implementation. Furthermore, the database containing information on firmware upgrades is not being kept up to date (see Figure 15).</p>
How it was supposed to be handled	<p>A firmware management governance is available to an extent to which firmware versions</p> <ol style="list-style-type: none">1) are regularly discussed target version between:<ul style="list-style-type: none">- System Architecture & Switch Vendor- System Architecture, Network Engineering and Switch Vendor through QBR meetings2) are evaluated & planned ad-hoc based-on recommendations and related applicable bugs provided by Extreme Network as part of regular alignments. Furthermore, potential new firmware version updates within skyguide's firmware upgrade are documented within skyguide's database (see extract Figure 15). The evaluation includes the identification of fixes, applicable for skyguide & new features from which skyguide can potentially benefit from. Once identified, a



	<p>decision is taken on how to further address bugs and new feature releases.</p> <p>3) are tested within a dedicated environment before being applied to production environment. This step includes the installation of the firmware version, the validation of its functionalities applicable for skyguide and the documentation of results.</p>
Interpretation	<p>According to our investigation,</p> <p>1) Regular meetings were conducted to discuss potential firmware level bugs and firmware level target versions, internally within System Architecture, Level 3 - Network Engineering and Level 2 - Network Operations as well as vendor Extreme Networks.</p> <p>2) Potential new firmware versions and related release notes were evaluated by skyguide's System Architecture and Level 3 - Network Engineering in terms of new features and in terms of bugs which might be applicable to skyguide. The process of implementing firmware was not completed on a regular basis, which would serve the purpose of ensuring continuous vendor support and technological debt avoidance. According to Figure 15, the last firmware upgrades approved by skyguide's firmware management governance were completed on 15th of November 2018 and later on 22nd of November 2022.</p> <p>Furthermore, it must be noted, that skyguide is not adhering fully to its internal processes of documenting firmware changes (Figure 15).</p> <p>3) Version 8.4.2 was tested by skyguide starting as of October 2021. During the tests, a critical bug was discovered. Thus, the version 8.4.2 was not considered as a valid firmware level. Our investigation further indicates that version 8.5.1 released in April 2022 was started to be tested in April 2022. New features like IP filtering, ingress map, bandwidth rating became available as part of version 8.5.1 which were considered as highly relevant for skyguide. It must also be noted that skyguide decided to skip version 8.4.3.</p> <p>During the implementation of firmware version 8.5.1 skyguide decided to shorten the validation period. While it is understood that after the incident of 15th of June 2022, the need to apply up to date firmware version was higher, the necessary time needed for firmware evaluation needs to be correctly assessed to allow both adequate testing results and process effectiveness.</p>



Conformity Level	Partially Conform
------------------	-------------------

Table 25: Conformity Analysis - Network Operation & Engineering: Firmware Management Governance

In general, is a network operation manual in place to ensure an efficient and effective network operation?	
Recap applicable Findings	As mentioned in chapter 3.6, as the Level 2 - Network Operations started the troubleshooting process of the incident on 13 th of June, there was no network operational manual available at this point in time.
How it was supposed to be handled	There is no network operation manual in place at skyguide. The operational manual shall provide the Level 2 - Network Operations with the necessary steps to manage and troubleshoot issues in an effective and efficient way.
Interpretation	The troubleshooting conducted by Level 2 - Network Operations did not rely on an network operational manual (as such does not exist). System warnings that appeared on 13 th of June 2022 were not further investigated to obtain the root cause.
Conformity Level	Not Applicable

Table 26: Conformity Analysis - Network Operation & Engineering – Network Operational Manual



In general, did skyguide follow its network escalation processes defined in its network operation governance / network operation manual?	
Recap applicable Findings	Level 2 - Network Operations was informed by Level 1 - SMC and started to investigate. Level 3 - Network Engineering was involved at a later stage.
How it was supposed to be handled	As stated in chapter 3.6, there is no formal escalation process in place to be followed by the Level 2 - Network Operations to involve Level 3 - Network Engineering during the investigation of the incidents of 13 th and 15 th of June 2022. As stated in various interviews, there is an informal agreement in place between Level 2 - Network Operations and Level 3 - Network Engineering. The escalation process shall ensure that events reported by network devices are addressed in an effective and efficient way.
Interpretation	As per its processes, Level 2 - Network Operations on-call in Zurich and Geneva was informed by its local Level 1 - SMC and started to troubleshoot. After some time, Level 3 - Network Engineering in Geneva was involved by Level 2 - Network Operations Geneva. Important to note is that Level 3 - Network Engineering is not obligated to be involved in a formal escalation process. As stated by Level 2 - Network Operations, there is only a so-called informal agreement in place between Level 2 - Network Operations and Level 3 - Network Engineering.
Conformity Level	Not Applicable

Table 27: Conformity Analysis - Network Operation & Engineering - Escalation process



4.5.2. Network Architecture and monitoring, HA and DR capabilities

This chapter analyzes the conformity of skyguide's network architecture and network monitoring capabilities.

Is skyguide's network architecture designed to fulfill skyguide's resiliency requirements?	
Recap applicable Findings	As described and explained in chapter 3.6, the incident occurred in ANS1 network. This is a physically independent network, which was build out of two network switch clusters, providing connectivity to all components connected to the ANS1 network.
How architecture is supposed to fulfill resiliency requirements	<p>From the holistic perspective, ANS1 network was designed to be fully redundant with ANS2 network, however the utilization of both networks depends on components connected to these networks and its configuration.</p> <p>Network setup follows network vendor's best practices from the time when it was deployed. One of the two network switch clusters in ANS1 network is composed of switch 09 and switch 10. This network cluster provides network connectivity for virtualized ANS applications hosted on VMware ESX servers to other parts of ANS1 network. The design of network switch cluster allows to provide resiliency on network switch level. Switch 09 and switch 10 were designed and implemented in a way to operate redundantly in case one of the devices stops functioning.</p>
Interpretation	<p>The investigation was focused on ANS1 network. However, it should be noted that skyguide has three separate networks in operation: ANS1, ANS2 and emergency network. Network architecture allows to utilize ANS1 and ANS2 as fully redundant networks. However, the redundancy must be properly designed for all components which are connected to ANS networks.</p> <p>During the investigation it was confirmed that only one system, which is responsible for radars, can utilize both ANS1 and ANS2 networks. Of all systems utilizing ANS1 networks, only the radar systems were not impacted by the incident on 15th of June 2022, because this system was able to automatically reroute the traffic through ANS2 network.</p> <p>The emergency network was designed to be used only as a last step to Clear-the-Sky. This network is not used if other methods are still available to complete the Clear-the-Sky procedure. Emergency network, per process design, cannot be used to support and maintain standard daily operations. The network investigation has shown that the network architecture was designed to provide redundancy on many levels. Redundancy is available on the</p>



	<p>physical device layer, the holistic network and logical redundancy for rerouting the traffic.</p> <p>However, the architectural design did not require connecting components to utilize ANS1 and ANS2 networks at the same time. This allowed the application components to utilize only half of the available network infrastructure and not to implement full available redundancy.</p> <p>The design also did not take into consideration additional checks, such as validating end-to-end data flows. This in turn did not allow the network teams to have a holistic picture of the health of the network, focusing only on components which the network vendor selected for monitoring.</p>
Conformity Level	Not Applicable

Table 28: Conformity Analysis - Network – Architecture

Is skyguide's monitoring solution to fulfill skyguide's resiliency requirements?	
Recap applicable Findings	<p>As described and explained in chapter 3.6, skyguide's network monitoring landscape consists of two independent solutions: XIQ and PRTG. XIQ (ExtremeCloud IQ) is a network monitoring tool provided by the same vendor which provided the network equipment – Extreme Networks. It is used by skyguide to provide network management, firmware management and analytics. PRTG is provided by Paessler AG. It is used by skyguide to perform trend analysis, utilization checks, bandwidth throughput and check load on CPU and network ports.</p>
How it was supposed to be handled	<p>As stated during the interviews, there is no formal guidance available which describes how Level 2 - Network Operations shall leverage its network monitoring solutions in an effective and efficient way. Network setup follows network vendor's best practices from the time when it was deployed, around year 2018. Monitoring infrastructure was set up using tools provided by the network switch manufacturer and popular and commonly recommended 3rd party monitoring software.</p> <p>The selected components should be designed & configured to allow an end-to-end network monitoring and visibility of all operations with a clear and easy to understand interface.</p>
Interpretation	<p>XIQ and PRTG monitoring tools are used independently and do not cover the same scope. This may lead to a single point of failure, as only one tool is monitoring the components. XIQ has shown problems with loading correct data for network devices during interviews. There is no redundancy provided for monitoring as the</p>



	two mentioned solutions have different monitoring scopes defined. In case of a monitoring system malfunction, information can be obtained only by directly connecting to each network device. Both tools do not provide a holistic overview of the network infrastructure to Level 2 - Network Operations. Information presented by the monitoring tools does not give a clear and easy to understand picture of what is happening in the network.
Conformity Level	Not Applicable

Table 29: Conformity Analysis - Network Monitoring

4.5.3. 13th of June 2022

This chapter analyzes the conformity of actions taken during the 13th of June 2022 by Level 2 - Network Operations and Level 3 - Network Engineering. As indicated in chapter 3.6, the first event to be considered as part of this investigation occurred on the 13th of June 2022.

Was the event acknowledged according to skyguide's internal guidelines?	
Recap applicable Findings	As described in chapter 3.6, the network error was detected on 13 th of June 2022 at 14:34. Level 1 - SMC contacted the Level 2 - Network Operations Team. As the on-duty team member was traveling, he connected to the monitoring solution XIQ and later connect directly to switch 10 at 15:57.
How it was supposed to be handled	Level 2 - Network Operations shall acknowledge and start troubleshooting a network event immediately once contacted by Level 1 - SMC. Level 2 - Network Operations on-call is composed of one network operator located in Geneva and one network operator located in Zurich. One of the network operators available on on-call shall have LAN expertise, a second Network Operator shall have WAN expertise.
Interpretation	The warning was acknowledged by Level 2 - Network Operations once contacted by Level 1 - SMC. Network status in monitoring tool XIQ was checked and investigation directly on switch 10 was started 1 hour and 23 minutes later. No impact on production environment was observed. This was in accordance with the internal processes.
Conformity Level	Fully Conform

Table 30: Conformity Analysis - Network Operation - 13th of June 2022 – SLAs



Was the investigation performed according to skyguide's internal guidelines?	
Recap applicable Findings	<p>As described in Chapter 3.6, the issue was acknowledged and started to be investigated by Level 2 - Network Operations. The investigation has shown that there were no clear guidelines available for Level 2 - Network Operations on how to handle such type of warning. Vlapc warnings were considered by the Level 2 - Network Operations as common at the time and were not causing issues in other parts of the network. XIQ monitoring tool provided by the network vendor was used to analyze the issue. In addition to the information available in the monitoring tool, network support connected as well directly to switch 10 to confirm information from the monitoring tool. Vlapc link on port 1/46 was reported as down, however the port itself was shown as operational and working correctly.</p> <p>It was decided to further monitor switch 10 and related network traffic for 15 hours. Afterwards the error was cleared from the monitoring system.</p>
How it was supposed to be handled	<p>There are no formal guidelines or requirement defined on how such topic shall be handled. The current situation is:</p> <ul style="list-style-type: none">- There is no network operation manual in place at skyguide. The manual shall provide the Level 2 - Network Operations with the necessary steps to address, manage and troubleshoot issues in an effective and efficient way.- The escalation process and related mandatory activities based on severity of the switch log entries are also not defined.
Interpretation	<p>During the investigation Level 2 - Network Operations team investigated the issue according to internal best practices. As the first step, the operational status of the affected port was checked using XIQ monitoring tool. Information available in XIQ was checked and considered as correct and up to date. XIQ tool was provided by the same vendor as the network equipment. As confirmed during the interviews, the skyguide's internal investigation report has shown that XIQ monitoring didn't show the correct status of switch 09 between 13th of June 2022 to 15th of June 2022.</p> <p>Level 2 - Network Operations were additionally crosschecking information about switch 10 from XIQ, to what was reported directly on the switch. However, investigation was not performed directly on the device which port 1/46 links to: switch 09. Switch 09 was shown as operating correctly in the monitoring tool. What was later found in the log, switch 09 reported the same issue as switch 10. However, this was not visible in XIQ monitoring tool and</p>



	<p>should be further assessed. Furthermore, the information available in PRTG tool was not verified.</p> <p>During the investigation on switch 10, the internal logs, ports statistics and interface status were investigated. However, the information about the increasing number of network packets errors was not highlighted and Vlapc root cause was not investigated further. Port statistics which have shown loss of data switch 09, which is connected via port 1/46, was not investigated by connecting directly the switch.</p> <p>After the investigation Level 2 - Network Operations implemented 15 hours of monitoring to ensure stability of the network. Afterwards, the warning message was closed without further investigation.</p> <p>The investigation was performed in accordance with the internal processes. The additional investigation check of verifying information directly on switch 10 didn't include checking the status on switch 09. Verifying information on both monitoring tools was not required by the process. This would allow Level 2 - Network Operations to address the issue, accordingly, potentially leading to further investigations (maintenance tasks, early engagement of switch vendor).</p>
Conformity Level	Not Applicable

Table 31: Conformity Analysis - Network Operation -15th of June

Was the event handled and resolved within the time frame set by skyguide's internal guidelines?	
Recap applicable Findings	As described in chapter 3.6, the network error was detected on 13 th of June 2022 at 14:34. Level 1 - SMC contacted the Level 2 - Network Operations Team. As the on-duty team member was traveling, he checked network status in XIQ and later connected directly to switch 10 at 15:57. Level 2 - Network Operations have completed the investigation on switch 10 at 16:21. The decision was made to further monitor the situation for additional 15 hours.
How it was supposed to be handled	As outlined during interviews, the Level 2 - Network Operations team troubleshoots error and warning messages reported by switch devices only to some extent. However, a formal guideline for troubleshooting is not formally defined and available at the time of writing this investigation.
Interpretation	During the event of 13 th of June 2022, Level 2 - Network Operations have completed the analysis with internally agreed timelines and additionally applied an extended monitoring time frame of 15



	hours. The monitoring period has not included performing additional steps which would allow to identify and understanding of the root cause.
Conformity Level	Not Applicable

Table 32: Conformity Analysis - Network Operation - Handling and resolution of issue

4.5.4. 14th of June 2022

This chapter analyzes the conformity of actions taken during the 14th of June by Level 2 - Network Operations and Level 3 - Network Engineering

On this day no specific alarms were detected, and no specific actions were performed in regard to the network devices which are in scope of this investigation.

Were the actions on 14th of June 2022 performed according to skyguide's internal guidelines?	
Recap applicable Findings	Level 2 - Network Operations and Level 3 - Network Engineering have not taken any additional actions regarding the event from 13 th of June 2022.
How it was supposed to be handled	Operational guidelines have no specific information on how to handle repetitive warnings, Vlapc related warnings, which monitoring tools and how the information needs to be verified, or when Level 3 - Network Engineering must be informed about specific warnings which are not causing an immediate impact on business services.
Interpretation	The event from 13 th of June 2022 was not further analyzed as it was assumed that network components were working correctly. Anomalies in the monitoring tools have not been detected by the configured alarms. The time available on the day of the 14 th of June was not used to perform maintenance activities on affected network devices or to perform deep dive investigations. Vendor was not engaged at this time to further analyze the root cause.
Conformity Level	Not Applicable

Table 33: Conformity analysis - Network Operation - 14th of June 2022



4.5.5. 15th of June 2022

This chapter describes the actions taken during the 15th of June 2022 by Level 2 - Network Operations and Level 3 - Network Engineering.

Was the event acknowledged according to skyguide's internal guidelines?	
Recap applicable Findings	As described in chapter 3.6, the network error was detected on 15 th of June 2022 at 01:07. Level 1 - SMC contacted the Level 2 - Network Operation Team at 01:15. First direct connection to switch 01 and 10 occurred at 01:45. At 01:57 the Level 2 - Network Operations WAN engineer in Zurich who was the investigation lead handed over the investigation to Level 2 - Network Operations LAN engineer in Geneva. At 03:39 Level 2 - Network Operations in Geneva have engaged Level 3 - Network Engineering in Geneva.
How it was supposed to be handled	Level 2 - Network Operations shall acknowledge and start troubleshooting a network event immediately once contacted by Level 1 - SMC. The Level 2 - Network Operation on-call is composed of one network operator located in Geneva and one network operator located in Zurich. One of the network operators on on-call shall have LAN expertise, a second network operator shall have WAN expertise.
Interpretation	The Level 2 - Network Operations acknowledged the warning reported by the Level 1 - SMC when contacted. Investigation on switch 10 was started 28 minutes later. Impact on production environment was confirmed. LAN engineer was engaged 42 minutes after the initial engagement of Level 2 - Network Operations. This was in accordance with the internal processes.
Conformity Level	Fully Conform

Table 34: Conformity analysis - Network Operation - 15th of June 2022 - Event Acknowledgement



Was investigation performed according to skyguide's internal guidelines?	
Recap applicable Findings	<p>As described in chapter 3.6, the issue was acknowledged and started to be investigated by Level 2 - Network Operations WAN engineer. Due to the complexity of the issue Level 2 - Network Operations LAN engineer from Geneva was engaged to investigate. Our investigation has shown that there were no clear guidelines available for Level 2 - Network Operations on how to handle this type of event.</p> <p>XIQ and PRTG monitoring tools were used to analyze the issue, however the tools didn't clearly show the exact root cause of the problem. It was determined during the interviews that XIQ and PRTG monitoring tools didn't have up to date and correct information from switch 09 since the event from 13th of June 2022.</p> <p>In addition to the information available in the monitoring tools, Level 2 - Network Operations connected directly to switch 01 and 10 at 01:45. First connection attempt to switch 02 failed at 01:58 due to invalid username and password combination. First successful connection to switch 09 was established at 02:55 and to switch 02 at 03:46.</p> <p>Switch 10 was reporting Vlapc link down on port 1/46 (connection to switch 09) since 13th of June 2022, however this warning was dismissed in the monitoring tool on the 13th of June 2022. Because of the alert dismissal, Level 2 - Network Operations didn't have a holistic picture of the network state. Same warning as on switch 10 was present on switch 09, however it was not visible in the XIQ monitoring tool.</p> <p>When switch 09 reported Vlapc link down on port 1/43 (connection to switch 01), the network traffic was rerouted via port 1/44 (connection to switch 02). This was the last available port to reroute the traffic coming from VMware ESX on switch 09. However, the successful rerouting of traffic via port 1/44 was not possible, as highlighted in Extreme Networks investigation (Extreme Case#:02612557, Chapter Second Incident @ June 15, 01:07 AM-03:20 AM, page 9). On port 1/44 the network traffic was dropped and unstable. At the same time the control plane for this port was still operating and reporting that the port is operational. This caused the switch 09 to be connected to the remaining part of the network with only one unstable link. The network switch itself and the monitoring tools did not report this state correctly.</p> <p>Level 2 - Network Operations investigated and connected to associated network devices in order find and analyze the root cause of the issue. Switch 02 was restarted at 03:25, followed by a reboot</p>



	<p>of switch 01 at 03:46. At 04:12 switch 02 was shut down and rebooted at 04:57.</p> <p>After further analysis of logs available on switch 09, it was decided to restart this network switch. Switch 09 completed the boot sequence at 05:03. This has stabilized the network and allowed to resume the connectivity between all network components. The team began evaluating stability of the network. Network stability was confirmed at 05:30.</p>
How it was supposed to be handled	<p>As outlined during interviews, the Level 2 - Network Operations and Level 3 - Engineering teams guidelines do not specify the way to address certain alerts and their related criticality. There is no network operational manual available at the time of writing this investigation, which would define the steps needed to address such situations. The escalation process and related mandatory activities based on severity of the switch log entries are also not defined.</p>
Interpretation	<p>During the investigation Level 2 - Network Operations team investigated the issue according to internal best practices and as an escalation step engaged Level 3 - Network Engineering in the troubleshooting process. The teams have checked information available in the XIQ and PRTG monitoring tools. Information available in XIQ was analyzed and considered to be valid. Switch 10 and later switch 09 were accessed directly to validate the available information. Approximately two hours were needed from the first direct connection to switch 09 to the time when a decision to restart switch 09 was made.</p> <p>The investigation was performed in accordance with the internal processes. Information which allowed to understand the root cause was not available directly in the XIQ monitoring tool and was not clearly labeled.</p> <p>Having correct information in the monitoring tools and being able to quickly analyze and understand crucial information and statistics would allow Level 2 - Network Operations to detect the issue on switch 09, potentially leading to faster decision to restart switch 09 and early engagement of network switch vendor.</p> <p>Being able to fully utilize ANS2 network and route all traffic from ANS1 to ANS2 would allow for much faster resuming of operations and would give network teams time to analyze the issue without impacting production workloads. Creation and ensuring that proper documentation and troubleshooting steps are available would allow for correct troubleshooting steps being applied. Having correct and up to date access to network equipment would allow for faster investigation times.</p>



Conformity Level	Not applicable
------------------	----------------

Table 35: Conformity analysis - Network Operation - 15th of June 2022 - Event investigation

Was the event handled and resolved within the time frame set by skyguide's internal guidelines?	
Recap applicable Findings	As described in chapter 3.6, the network error was detected on 15 th of June 2022 at 01:07. Level 1 - SMC contacted the Level 2 - Network Operations Team at 01:15. The investigation was started and first direct connection to the network devices was made at 01:45. Level 3 - Network Engineering was engaged at 03:39. The investigation and successful problem resolution was confirmed at 05:30.
How it was supposed to be handled	A guideline for troubleshooting steps performed by Level 2 - Network Operations and Level 3 - Network Engineering is not formally defined and available at the time of writing this investigation report.
Interpretation	During the event of 15 th of June 2022 Level 2 - Network Operations have completed the analysis and escalated the issue to Level 3 - Network Engineering with internally agreed timelines. During the investigation crucial information from switch 09 was not discovered in a reasonable timeframe to allow for an immediate decision to restart the switch 09. Ensuring defined SLA guidelines and escalation procedures are available would allow for quicker engagement of Level 3 - Network Engineering and their expertise or to engage troubleshooting steps as per predefined operating procedures to isolate the equipment which is considered as impacted.
Conformity Level	Not applicable

Table 36: Conformity Analysis - Network Operation - Handling and resolution of issue

4.5.6. Summary of events / conclusion

The objective of this chapter is to summarize from a technical point of view the relevant events within ANS1 network, focusing on affected network devices: switch 09 and switch 10. For this purpose, the root cause analysis of the switch vendor will be considered.

The overall design principles required to understand the nature of the problem are outlined below.

Network communication uses service hierarchy of protocol layers. Each of the layers provides a set of guaranteed services to the layer above it. The layer above is operating by making assumptions about all lower-level transport services. The protocol stack consists of seven protocol layers.



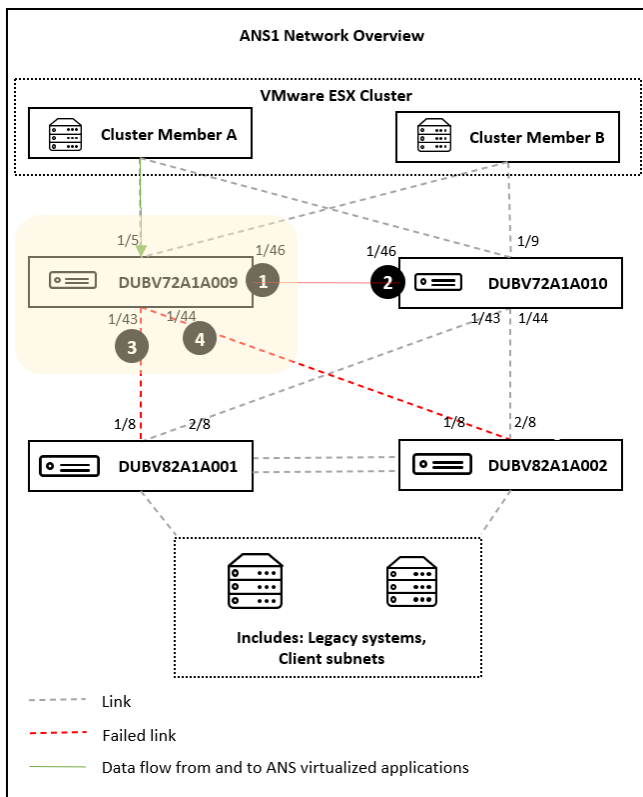
The network switches provided by the vendor Extreme Networks have a Quality of Service (QoS) feature. This component has seven queues, where the highest has the highest priority.

The network switch high-level design consists of a CPU control plane and a switching ASIC data plane. The data packets which are received by the network switch are sent directly to the ASIC, without CPU involvement. The network control plane packets, for example Vlacp, are sent over QoS queue seven, in order to provide and ensure network stability.

As outlined and summarized in Extreme Network's Case#:02612557 "Skyguide Root Cause Analysis", switch 09 experienced Vlacp link being down, which was resolved after the network switch reboot. The first link which became down was on port 1/46, which is connected switch 10. This is shown as (1) and (2) in Figure 7. Network traffic was automatically routed around the failed link. This occurred on 13th of June 2022 at 14:34. The historical data available in PRTG monitoring tool confirms that that the network traffic was stopped on this port. The network switch vendor analysis confirms that the physical

layer was still operational, however the network packets were being dropped. This can be seen in the network switch port statistics. The lack of data transmission caused switch 09 and switch 10 to disable the Vlacp link between them.

On 15th of June 2022 at 01:07 Vlacp link on port 1/43 linking to switch 01 became down (3) and is visible in the number of dropped packets on QoS queues zero, one, six and seven. This caused the network switch 09 to have only one remaining link route to the remaining part of the network. Switch 09 automatically rerouted the network traffic through the last available port 1/44 which is linking to switch 02, however this port was operating only partially (4). The partial operation of the port is visible in port statistics, where QoS queues zero and one have shown network packets loss. The packet loss was at a level which still allowed some network communication to still be sent correctly, as confirmed during the interviews and visible in



13th of June 2022

- ① 14:34: DUBV72A1A009 - Vlacp Link 1/46 is down (not visible in monitoring tools)
- ② 14:34: DUBV72A1A010 - Vlacp Link 1/46 is down

15th of June 2022

- ③ 01:07: DUBV72A1A009 - Vlacp Link 1/43 is down
- ④ 01:07: DUBV72A1A009 - Vlacp Link 1/44 is shown as up however data is not sent

Figure 7: Overview Network



PRTG port monitoring logs. As outlined by the vendor's root cause analysis, the control plane on port 1/44 continued to operate. The control plane has maintained port 1/44 status as operational, however not all data was being transferred due to the errors. Errors which caused packet loss occurred only on lower level QoS queues and the control plane traffic was not impacted.

Furthermore, the network vendor's root cause analysis suggested with high probability that if switch 09 would have been rebooted on 13th of June 2022, the incident on 15th of June 2022 would not have occurred. It is worth noting, however, that this would not have resolved the root cause of the problem and potentially it could have only delayed the problem from occurring. The network switch was not designed to detect this type of problems and the implemented monitoring solutions also were not designed to validate end-to-end network connectivity. Extreme Networks stated that the network switch reboot would not cause an outage. However, as confirmed during interviews, skyguide's application stack does not allow for network switch reboot without an impact on applications. This has not been configured, even though on network level another network switch can automatically take over the traffic from the switch which is being rebooted.

Similar cases were reported by other Extreme Networks customers, as highlighted in Extreme Network's Case#:02612557 "Skyguide Root Cause Analysis". This indicates a probable issue with firmware versions released before versions 8.0.8 and 8.1.2, which are available since February 2020.

As a part of the QBR on 22nd of February 2022, Extreme Networks provided two new firmware versions available for the affected network switch model. The first firmware version is the Maintenance Release, which is the official last firmware version supported for bug fixing. The Latest Feature Release is the most recent firmware version, which additionally to the bug fixes provided in the Maintenance Release, it provides latest new features. The presented firmware versions were 8.4.3.0 for Maintenance Release and 8.5.0.0 as Latest Feature release. Firmware version 7.1.0.0 is not officially supported anymore since the release of version 8.1.1 in January 2020.

Skyguide benefits from Extreme Premier Support Contract, which allows them to still receive support from Extreme Networks for firmware versions older than the minimum maintenance release version. The selected approach to apply firmware releases is considered to be very safety driven. Skyguide uses reactive approach to applying new firmware versions in order to avoid introducing unwanted changes, downtime and firmware bugs which were not yet discovered. This has resulted in skyguide not having firmware implementations since November 2018, omitting opportunities to upgrade firmware over the course of the past four years (eg. Version 8.0.8).

Skyguide has updated its firmware upgrade strategy in October 2021, when it was decided to upgrade from version 7.1.0.0 to version 8.4.2. Due to discovered critical bugs this had to be cancelled and decision was made to wait until version 8.5.1 is available. The exact point time of this decision is not logged in the database containing information on



firmware upgrades (see Figure 15). At that point in time skyguide was deemed to wait for version 8.5.1 without other alternatives. Tests of version 8.5.1 began shortly after its release in April 2022, and it was decided to shorten the six months test cycle, which was last used in 2018 during 7.1.0.0 implementation.

The root cause analysis provided by Extreme Networks to skyguide states, that there are indications that updates in newer firmware versions may provide some benefits. The network switch vendor outlines that firmware version 8.0.8 and 8.1.2 released in February 2020 address a queue overflow condition on a shared memory pool counter, which stops traffic on affected queues and ports. It was pointed out by the network switch vendor's root cause analysis, that the firmware fix for this issue applied an active monitoring of ASIC switching queues and can take reactive measures to automatically clear the failure condition. As a conclusion, the switch vendor recommended to upgrade firmware level to release 8.5.1. or later. This recommendation is being applied by skyguide on their network devices at the time of writing this document. However, it must be noted that skyguide has not kept the firmware level up to date for a long period of time on the affected network switches and considerably shortened the firmware testing period during 8.5.1 implementation.

The network switch vendor has additionally recommended network switch replacement. This task was completed by skyguide, however, as of the time of writing this report, Extreme Networks has not contacted skyguide after receiving the network switch for further analysis.



5. Conclusion

This chapter contains an answer to each question listed in the book of specification.

- Chapter 5.1 provides a brief overview of actors and events
- Chapter 5.2 provides an answer for each question as per the book of specification related to network.
- Chapter 5.3 contains an answer for each question as per the book of specification related to crisis management.



5.1. Overview

The following figure shows an overview of all events and related actors.

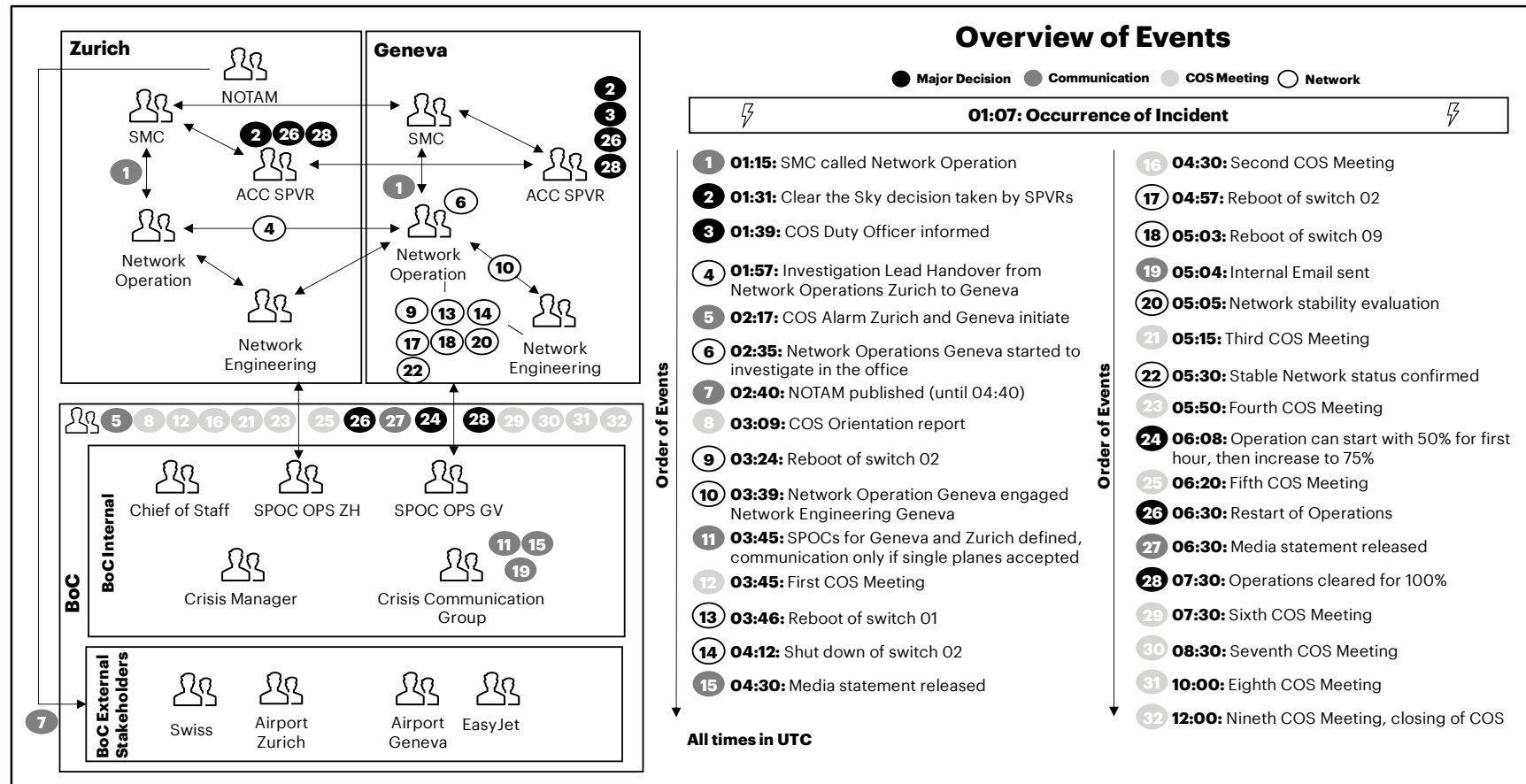


Figure 8: Overview and Sequence of Events (UTC)



5.2. Network

In particular, the following questions were answered during the investigation:

Question 1: What exactly was the technical problem and what was the cause?

One network component of a central switch cluster used at skyguide came out of synch which resulted in network degradation. The misbehavior of that component later increased. The network switch was reporting as still operational, even though the key functions of handling network traffic had failed. This caused a major network disruption affecting applications used for Air Navigation Services.

Our analysis of the provided logs for the network cluster (consisting of multiple devices) between the 13th and the 15th of June 2022 have shown that certain circumstances have led to the major incident which occurred on the 15th of June 2022 (see chapter 3.6 Figure 6 and chapter 4.5.6 Figure 7).

On the 13th of June 2022, switch 09 and switch 10 reported at 14:34 that Vlapc link on port 1/46 is down. This port functions as an inter-switch-link used to connect switch 09 and switch 10. This has not impacted the application services, as redundant connections were still operational and could be successfully utilized. The ports were still shown as operational. As already outlined in skyguide's internal report, the error was captured by Level 1 - SMC team in Zurich, and a ticket was opened with the reference I220613_0048. The root cause analysis by the switch vendor confirms that the network devices successfully re-routed traffic around the failure.

On the 15th of June 2022, 01:07, switch 09 and switch 10 reported that Vlapc link 1/43 is down, resulting in disabling the port for higher protocols, as confirmed by the switch vendor's root cause analysis. Additionally, Vlapc link on port 1/46 was still down on switch 09 and switch 10, however this alarm was cleared from XIQ monitoring tool on 13th of June 2022 and not visible anymore.

The XIQ tool reported at 01:07 a significant number of alerts, which needed to be investigated by Level 2 - Network Operations. At this point in time, the link on port 1/44 originating from switch 09 destined to port 1/8 on switch 02 was still reported as operational. The root cause analysis of the switch vendor outlines that a partial impact on port 1/44 on switch 09 was not detected by the switch 09. Furthermore, drop packets on switch 09 port 1/44 were reported for QoS queue 0 and queue 1 (used for application traffic), but not on queue 7 (used for the control plane traffic like Vlapc, vIST and IS-IS). Switch 09 port 1/44 was determined as operational by the switches control plane and by neighboring network devices. The switch vendor confirmed that, at that point in time, data being transferred between switch 02 and 09 was dropped by switch 09. This was further confirmed in the network switch logs analysis and in the historical data of PRTG monitoring tool (see Figure 12, Figure 13, Figure 14).



The incident on network switch 09 caused a network disruption. The forwarding of network traffic was impacted. The fact that switch 09 was still being able to process certain higher-level protocols on last remaining operational port connecting to other parts of the ANS1 network, didn't trigger a clean failover to its redundancy partner switch 10. The clean failover allows another network device to take over the network traffic from the failed device and maintain network status as operational.

As indicated by network switch vendor Extreme Networks, the fault could be a result of a firmware bug or a hardware malfunction. The data to confirm exact cause is not conclusive and only allows to confirm which network device caused the outage.

Question 2: Was the event predictable?

The network event which occurred on the 15th of June was predicable in terms of further Vlacp link issues, network degradation and a potential network disruption. Network events on switch 09 and switch 10 already reported on 13th of June 2022 were not effectively and efficiently addressed. An Operational Network Handbook should have given clear instructions on how to approach the network disruption symptoms.

Our analysis has shown that first issue on the network switch which caused an outage on 15th of June 2022, occurred on the 13th of June 2022. Two network devices (switch09 and switch10) reported that Vlacp link was down on port 1/46. This error was detected by Level 1 - SMC monitoring on switch 10 and XIQ monitoring. Level 2 - Network Operations checked the status of the port on switch 10. Switch 10 reported to XIQ monitoring tool that link is down and that the port is still operational. Switch 09 was reported in XIQ to be operating correctly. The changes in network traffic were not investigated in depth using skyguide's second monitoring tool, PRTG (see Figure 12 and Figure 13).

As a conclusion, it was decided to continue monitoring the health of this switch and related port for the next 15 hours before closing the incident. There was no further data collection taken and analyzed with the related switch vendor which might have given further indications and potential mitigations. Information from switch 09 was not verified and traffic flow monitoring was not verified in PRTG.

The log message has been sent with the severity "warning". Unfortunately, there is no operational network handbook in place that instructs Level 2 - Network Operations the required actions based on the log severity. Due to the absence of the network operation manual, there was no basis for a full understanding of the error and the



associated pressure to act. *Therefore, an operational network handbook might reduce the risk of incidents, and the aggravation of incidents.*

Nevertheless, it must be emphasized that there's a need for network redundancy utilization on application level, as well as for training and knowledge sharing within and between the teams.

The firmware version 7.1.0.0 installed on the affected network switches was verified by skyguide and was considered as stable (see Figure 15). No firmware related issues which would demand firmware version change had been reported internally since implementation. All network devices completed scheduled maintenance tasks successfully. While firmware upgrades were recommended by the network switch vendor Extreme Networks, there hasn't been any specific indications during the QBR, that such a failure could occur and cause a major incident.

Question 3: Has skyguide initiated the right technical remedial measures at the right time and quickly enough?

The analysis has shown that the teams involved in the investigation of the network incident which occurred on 15th of June 2022 were delayed in the analysis due to missing knowledge to interpret data shown in the monitoring tools, complex documentation structures and the key information not being available at hand.

The first escalation process initiated from Level 1 - SMC to Level 2 - Network Operations worked successfully in the expected time frame, allowing for quick engagement of the on-call engineer of Level 2 - Network Operations. The Level 3 - Network Engineering was engaged two hours and 24 minutes after Level 2 - Network Operations was engaged.

As already outlined in question 2, the operations personnel could have acted differently on 13th of June 2022 with a respective operational network handbook in place and clear instructions for addressing log entries categorized as warning and error. A more comprehensive description of the recommendations for follow-up activities are described in chapter 6.

At 14:34 on 13th of June 2022, the monitoring of Level 1 - SMC started to report a failure on network switch 10. Level 1 - SMC has contacted Level 2 - Network Operations, who started the analysis. Level 2 - Network Operations investigated the issue by using XIQ monitoring tool and later at 15:57 connected directly to switch 10 for further investigation. The network monitoring tool XIQ was only showing an issue on switch 10 and was not reporting an issue on switch 09. Information showing loss of data



transmission on related ports in PRTG monitoring tool was not investigated. Based on gathered information, Level 2 - Network Operations concluded that all ports were up and running and the network is operating normally. It was decided to continue monitoring the health of the network and related port for the upcoming 15 hours before closing the incident. There was no data collection taken for switch 09 and no further data collection generated for switch 10 for further switch vendor analysis. Furthermore, data flow changes were not checked and analyzed in PRTG monitoring tool.

At 01:07 on 15th of June 2022, the monitoring of Level 1 - SMC started to report a major failure for many applications. Within minutes Level 1 - SMC has reported the incident to the on-call of Level 2 - Network Operations, who started the analysis. After initial analysis, second Level 2 - Network Operations colleague was asked by the on-call colleague to support at 01:57.

Assessing the large impact, one of the Level 2 - Network Operations team members travelled from home to the datacenter to be able to support locally. Level 2 - Network Operations Geneva arrived at the office at 02:35. Level 2 - Network Operations decided to escalate and ask for support from Level 3 - Network Engineering at 03:39. Despite the call being placed outside the service hours for Level 3, Network Engineering answered the call. Level 3 - Network Engineering are not required to answer calls outside of standard working hours.

The Level 2 - Network Operations and Level 3 - Network Engineering, both teams present at this point in time remote as well as onsite in Dübendorf and Geneva, were narrowing the incident by starting to reboot switches in close alignment with Level 1 - SMC. Unfortunately, neither the alternate reboot, nor the isolation of switches 01, 02, 03 and 04 resolved the issue.

Remote connection to switch 09 for investigation purposes was delayed due to failed attempts. The failures were caused by unstable network connection. After establishing a successful connection switch 09 was investigated and was highlighted as the problem root cause. Before the switch could be rebooted as a measure to resolve the issue, logs from the device had to be obtained. Downloading the logs through a remote connection was not performing as expected and was later abandoned in favor of connecting physically to the network switch. Direct connection allowed to obtain the logs in a standard timeframe and to proceed with network switch reboot.

The reboot allowed the network switch to rebuild its full functionality. Level 2 - Network Operations and Level 3 - Network Engineering tested the functionality of the network for 30 minutes before confirming the network as fully operational again.



Question 4: Were the processes by which the remedial action was initiated in place, adequate and effective?

The processes to detect and escalate network incidents is in place at skyguide. These processes are adequate to engage Level 1 - SMC and Level 2 - Network and were effectively executed on 13th and 15th of June 2022. However, the Level 3 - Network Engineering are not required to answer calls outside of standard working hours, as this team does not provide on-call support. In case Level 3 - Network Engineering would not have answered the call, the network outage on 15th of June 2022 could have lasted longer. The network operating manual for the Level 2 - Network Operations on how to troubleshoot and resolve such cases were not in place. Skyguide relies on the knowledge of its personnel for such issues.

During the night of the 15th of June 2022, the Level 1 - SMC was unable to resolve the problem by himself. In such cases Level 1 - SMC contacts the on-call for Level 2 – Network Operations. On-call in Zurich and Geneva were both contacted by the Level 1 - SMCs, at 01:15 and 01:19 respectively. The on-call Level 2 - Network Operations were available as expected. The support model does not include the availability of Level 3 - Network Engineering team. Given the severity of the situation on the 15th of June 2022, Level 2 - Network Operations contacted and escalated the issue to Level 3 - Network Engineering at 03:39.



Question 5: Were maintenance procedures in place, were they applied and were they effective? Should the updates made now, have been done earlier?

Question 5a: Were maintenance procedures in place, were they applied and were they effective?

Technical and organizational maintenance procedures are in place at skyguide. From hardware installation and maintenance perspective, they are actively, regularly, and effectively used. However, in this specific case, the process of maintaining firmware levels failed to address the upgrade on time.

The quarterly service review meetings established between skyguide and network switch vendor Extreme Networks follows an organized structure. These meetings include installed hardware and end of support life hardware review, open case review, open support and sales topics, which is followed by recommended software and communication topics. While the network switch vendor provides their recommendations, skyguide makes the final decision on what is implemented and when. The business that skyguide operates requires stability and this is the main objective for Level 2 - Network Operations and Level 3 - Network Engineering. This priority has focused skyguide's decision making process on avoiding introducing unnecessary changes, which might impact stability of the environment.

The firmware version 7.1.0.0 installed on the affected network switch was running stable since 2018. Skyguide has not applied new firmware releases before the incident which occurred on 15th of June 2022, as described in chapter 4.5.6.

From an organizational point of view, skyguide has established and maintained a firmware management governance including firmware analysis, firmware strategy and firmware testing. However, they have omitted opportunities to upgrade firmware over the course of the past four years. The Level 3 - Network Engineering is responsible for firmware level governance of switches within all networks, while Level 2 - Network Operations execute firmware upgrades according to the predefined firmware management governance. While the firmware upgrade project can be highlighted by Level 3 - Network Engineering as required, it is possible that it will not be considered and planned by skyguide during prioritization.

From hardware point of view, the maintenance procedures for managing the network hardware, network cabling and electricity are in place and are effective. Hardware is being tested, network switches are restarted on a yearly schedule, power redundancy is tested and evaluated.



5b) Should the updates made now, have been done earlier?

The network switch firmware version 8.0.8 and 8.1.2 released in February 2020 address a queue overflow condition on a shared memory pool counter, which stops traffic on affected queues and ports. Had an update between March 2020 and mid-June 2022 been executed, it most likely would have prevented the 15th of June 2022 network incident. However, it is worth noting that the issue has affected only on one out of four network switches working in this configuration. The exact condition which triggered the fault was not confirmed by Extreme Networks. The fault could have been caused by a bug in the firmware or a hardware malfunction.

Firmware upgrade cycles at skyguide have prioritized network stability. New firmware versions were not required to accommodate new business requirements, until the planned implementation of firmware version 8.4.2 in October 2021. As part of the QBR meeting between skyguide and Extreme Networks which took place on 22nd of February 2022, firmware version 8.4.3.0 was highlighted by Extreme Network as maintenance release (minimum release level supported by the switch vendor for bug fixing) and version 8.5.0.0 as latest feature release (latest firmware available including the latest features successfully tested) (see Figure 11). The planned release of firmware version 8.4.2 has been cancelled by skyguide due to discovered critical bugs and version 8.5.1 was selected as the next candidate for deployment. This firmware version was made available by Extreme networks in April 2022. However, the decision to upgrade to version 8.5.1 was not taken before the incident occurred.

The time testing period, which has been shortened during 8.5.1 release, if it would have been shortened at earlier stage, it could have allowed skyguide to implement previous firmware releases and potentially avoid the 15th of June 2022 incident.

The applied risk avoidance has led to delayed firmware upgrade process. The firmware version 8.0.8 and 8.1.2, which addresses this type of issue, has been available for over two years. This time should have been used to complete necessary validations and implementation.

It was pointed out by the switch vendor's root cause analysis, that the firmware fix provided by version 8.5.1 for this issue applied an active monitoring of ASIC switching queues and can take reactive measures to automatically clear the failure condition. As a conclusion, the switch vendor recommended to upgrade firmware level to release 8.5.1 or later. This recommendation is being applied by skyguide on their network devices at the time of writing this document.



Question 6: Did the technical infrastructure allow the correct remedial measures to be identified?

The affected network switches 09 and 10 have detected an issue on 13th of June 2022. Monitoring system picked up the information from switch 10 and triggered an incident. A proper operational network handbook, extensive knowledge of the network environment landscape and end-to-end-monitoring systems would have helped to handle the incident more effectively and efficiently.

The monitoring, as a critical element, is currently established as re-active only and the available monitoring solutions disclose potentials for improvements. An end-to-end-monitoring solution enriched with automation can potentially detect anomalies before an incident occurs.

Details to what could have been handled differently on 13th of June 2022 has already been described in question 2.

From our experience, one of the crucial capabilities to initiate actions in an appropriate manner are holistic and end-to-end monitoring capabilities. Skyguide's current monitoring landscape consists of various tools. On a first level, iSUP is used by System Monitoring and Controlling. On Level 2, domain-specific products are being used: XIQ and PRTG are used by Network Monitoring.

iSUP is used to detect and triage events captured by various IT devices. Initial analysis indicates that this platform offers a wide range of reactive capabilities but does not offer the ability to trace certain data flows end-to-end and to predict certain events based on historical data sets. During the incident of the 15th of June 2022, Level 1 - SMC received many events captured from different layers (application, servers, network, etc.). Furthermore, our analysis showed that it was very time consuming to correlate the huge number of events reported by various IT devices in iSUP without any end-to-end application and data flow monitoring capabilities.

Given the situation described above and its limitations, our investigation indicates that skyguide's technical infrastructure in terms of operational monitoring and tooling did not provide clear oversight in order to identify and apply correct remedial measures quickly and effectively. However, it must be highlighted, that PRTG monitoring tool allowed to check information regarding network traffic, which would allow for quicker root cause analysis. Additionally, monitoring tools XIQ and PRTG didn't display fully correct information regarding switch 09, due to the nature of the problem.



Question 7: Has the functional behavior in degraded modes been predicted and specified?

Skyguide has a procedure in place for applying degraded mode of operation. However, the guidelines, checklists, and processes to not specify how to apply these in case of such a Swiss-wide and complex root cause of a problem.

As already outlined in chapter 4, a proper governance is in place applying skyguide's mode of operation in specific circumstances. In the event of the 15th of June 2022 and considering the nature of complexity and impact of the problem, the guidelines described in skyguide's degradability-handbook was not applied by supervisor as Level 1 - SMCs were not able to triage the root cause of the problem and to predict the approximate resolution time.

Thus, the supervisor decided to initiate a Clear-the-Sky procedure. It has to also be noted that there is not a clear mapping of application to underlying technology landscape available which may have helped Level 1 - SMC to initially triage and correlate events in an effective and efficient way.

Question 8: Was there enough redundancy in the technical infrastructure that had a malfunction?

Skyguide is operating most of its critical ANS applications within a single fully redundant network. The network infrastructure is built on a primary and secondary switch and the servers are connected to both switches. This configuration has been built according to best practices.

Our observations indicate a lack in definition of the business continuity & disaster recovery requirements (in terms of Recovery Point Objective and Recovery Time Objective) to IT Service Level Agreements (IT SLAs). With SLA in place, IT has clear specifications on how to build services and redundancies to meet or exceed the SLA's.

Furthermore, a lack of a BCM (Business Continuity Management) and DR (Disaster Recovery) plan was observed, that specifies which hazards IT services must sustain. Whether the built-in redundancy is sufficient for the business, can only be confirmed if SLA's and BCM/DR plans are in place.

The network components in the ANS network are built on multiple switches connected in a full mesh design. A full mesh design allows for some switch-to-switch connections



to fail without having an impact on the service availability or the performance. This redundancy also takes into consideration scenarios where whole single network components fail. The configured protocols identify the faulty connection and re-route the traffic to its redundancy. This design is acknowledged as good practice.

However, the redundancy from a holistic perspective must be further investigated. Application and server layer were not in scope of this investigation. From a holistic view, it was discovered during this investigation, that the network services offer resiliency by providing two fully independent networks ANS1 and ANS2. The connecting components are not mandated to utilize this resiliency. It is worth noting that utilizing this redundancy in full scope, could have prevented the 15th of June 2022 incident from occurring. As confirmed during the conducted interviews, ANS applications are not leveraging the resiliency provided by the network layer.

Question 9: Were the methods for analyzing the architecture appropriate?

This question is partially answered in questions 6 and 8. The methodology applied by skyguide for investigating and troubleshooting network related incidents is based on engineers' best knowledge. Operating instructions addressing this type of issue were not available at the time of writing this document. Skyguide has not defined measurable business requirements for network components.

Business requirements must be further assessed and translated into IT Service Levels (SLA). Furthermore, there is a lack of a Business Continuity Management (BCM) and Disaster Recovery (DR) plan that specifies which hazards IT services have to be able to sustain. Operating instructions would allow Level 2 - Network Operations for faster issue resolution.

Question 10: Did the analysis identify individual architectural failure points?

This question is partially answered in questions 8 and 9. The ANS network architecture follows best practices provided by the network switch vendor from the point of implementation.

While the ANS network architecture allows to achieve many levels of redundancy, this must be further assessed on application and server level, which are not in scope of this investigation. A higher availability of the systems can be achieved by configuring ANS application layer to fully utilize available ANS networks. As this may require a significant financial and resources effort, it is suggested to investigate into a contractual alignment between business and IT as described in questions 8 & 9.



Question 11: Was the redundancy analyzed and was it appropriate for the decoupling (“isolation”) of the systems?

This question is partially answered in questions 8, 9 and 10. The redundancy of the analyzed switch cluster is according to best practices provided by the network switch vendor from the time of implementation. An increase of the redundancy is possible and can be achieved by implementing additional redundancies on network switch cluster level within ANS1 and ANS2 networks.

Whether this is required and beneficial for the business operations has to be further assessed, confirmed and verified with exact business requirements. Based on this decision, appropriate IT SLAs shall be derived for skyguide’s IT landscape.

The redundancy of the deployed network switch clusters is implemented according to best practices provided by the network switch vendor from the time of the implementation. As elaborated in previous answers, the additional redundancy requirement needs to be further assessed with business requirements and incorporated into IT SLA. The incident which occurred on 15th of June 2022 has affected ANS1 network and allowed services such as radar and telephony to operate normally using ANS2 network. The design of separate networks is typically applied for the highest availability but requires an assessment about additional investments and effort to uplift the applications.

Our investigation has shown that two independent networks exist with ANS1 and ANS2. The affected switches 09 and 10 are part of ANS1. The servers used to provide ANS application services are only utilizing ANS1 network and are not utilizing any switches from ANS2 network. Another important finding was that ANS1 and ANS2 networks are composed of switches physically installed in Dübendorf, but not geographically distributed to Geneva.



Question 12: How can such a situation be prevented in the future?

Our investigation concluded that such an event may be prevented in the future by organizational and technical capability improvements, which need to be further assessed in detail.

As part of this investigation, the incident was analyzed not only from a technical but also from an organizational point of view, focusing on the network layer part. As stated in chapter 1, application- and server layer were not in scope of this investigation and should be further assessed more in detail.

*From a **technical point of view**, our investigation identified some potentials to further improve skyguide's technical capabilities. One of the major potential improvements identified during our investigation was skyguide's end-to-end-Monitoring capabilities. As outlined in chapter 3, skyguide's current end-to-end monitoring solution used by Level 1 - SMC only contains reactive, but not predictive and data-flow-driven capabilities. Such capabilities may have helped Level 1 - SMC to correlate different events provided by various data sources and to identify the root cause of the problem in a more efficient manner.*

*From an **organizational point of view**, a comprehensive network operation manual may have helped skyguide to ensure that events on network devices are handled and troubleshooted in an appropriate effective and efficient way. For example, ensuring that events categorized as error and warnings have to be managed in an appropriate way and may involve switch vendor support in a very early stage.*

In summary, further assessments shall be conducted to evaluate not only organizational depth and breadth, but also to identify potential improvements in monitoring. Please refer to the recommendation chapter for detailed information.



Question 13: How can similar situations be identified at an early stage?

To provide early-stage identification of similar network disruptions, as described in previous answers, a holistic monitoring solution should be implemented, operating instructions and adequate training provided to Level 2 - Network Operations and Level 3 - Network Engineering. To ensure that the issue is handled within agreed timelines, business requirements must be translated into IT Service Levels in the first step to define what service degradations can be accepted by the business. The definition of IT SLA will allow IT to define the required actions.

Skyguide possesses only re-active monitoring capabilities. A further analysis is proposed to develop an end-to-end monitoring concept including predictive maintenance and automation.

Please refer to previous questions and the recommendation chapter for detailed information.

Question 14: The results of skyguide's internal investigation should also be questioned: Does the gathered information confirm the results of skyguide's internal investigation (technical reports / safety investigation report) or not?

The skyguide internal investigation report has been comprehensively developed and is clearly structured. The conducted investigation confirms skyguide's internal investigation and highlights additional improvements, as further discussed in chapter 7.

The review of the internal report confirms our made observation in general. This independent investigation has identified additional improvements that shall be further assessed to mitigate the risk for similar incidents. The recommendations are described in chapter 6.

Please also refer to chapter 7 for the appraisal of skyguide's investigation report.



5.3. Crisis Management

In particular, the following questions were answered during the investigation:

Question 15: Has the COS process (Crisis Organization skyguide) been adhered to?

Our external investigation concluded that the COS process was mostly adhered to. There were some minor issues in escalation and execution of the process. Yet, those findings were not impacting the successful mobilization and execution of the process which led to the resolution of the technical issue within 5 hours. The frequent training of the COS process has shown its intended impact on structured and professional resolution in this case.

A detailed description about the escalation and execution of the COS process can be found in chapter 3.5 and 4.4.

Question 16: What was the collaboration, communication and decision-making process like within the COS team?

Based on interviews with members of the COS, the external investigation has shown that the roles were clearly defined. The conducted COS meetings were structured as per the defined agenda. SPOCs were defined to communicate information into the Common IFR Rooms. Additional information required could be requested to the responsible team. The situation in the Common IFR Rooms was described as calm and organized. The decision-making process was described as evidence based.

A detailed description of the collaboration, communication and decision-making process can be found in chapter 4.4.



Question 17: In their own opinion, have the stakeholders (internal/external) been sufficiently informed?

Skyguide has performed internal qualitative and quantitative analysis on how the communication efforts have been perceived. They concluded that the various information needs of their various stakeholders have been met well, but identified certain points of improvements. During our external investigation a review of the internal analysis and interviews with stakeholders were conducted. The stakeholders interviewed were satisfied with the communication they had received on the 15th of June 2022. Improvements were identified as outlined in chapter 6. Skyguide's internal analysis was detailed and outlined lessons learned regarding communications. As mentioned in chapter 7, these can be confirmed by the present investigation.

A detailed description of the information received in their own opinion can be found in chapter 4.2.



6. Recommendation

This chapter summarizes the recommendations and conclusions based on findings described the previous chapters. During this investigation, the following **area for improvements** were observed which are structured along key parts applicable for this investigation shown in Figure 9:

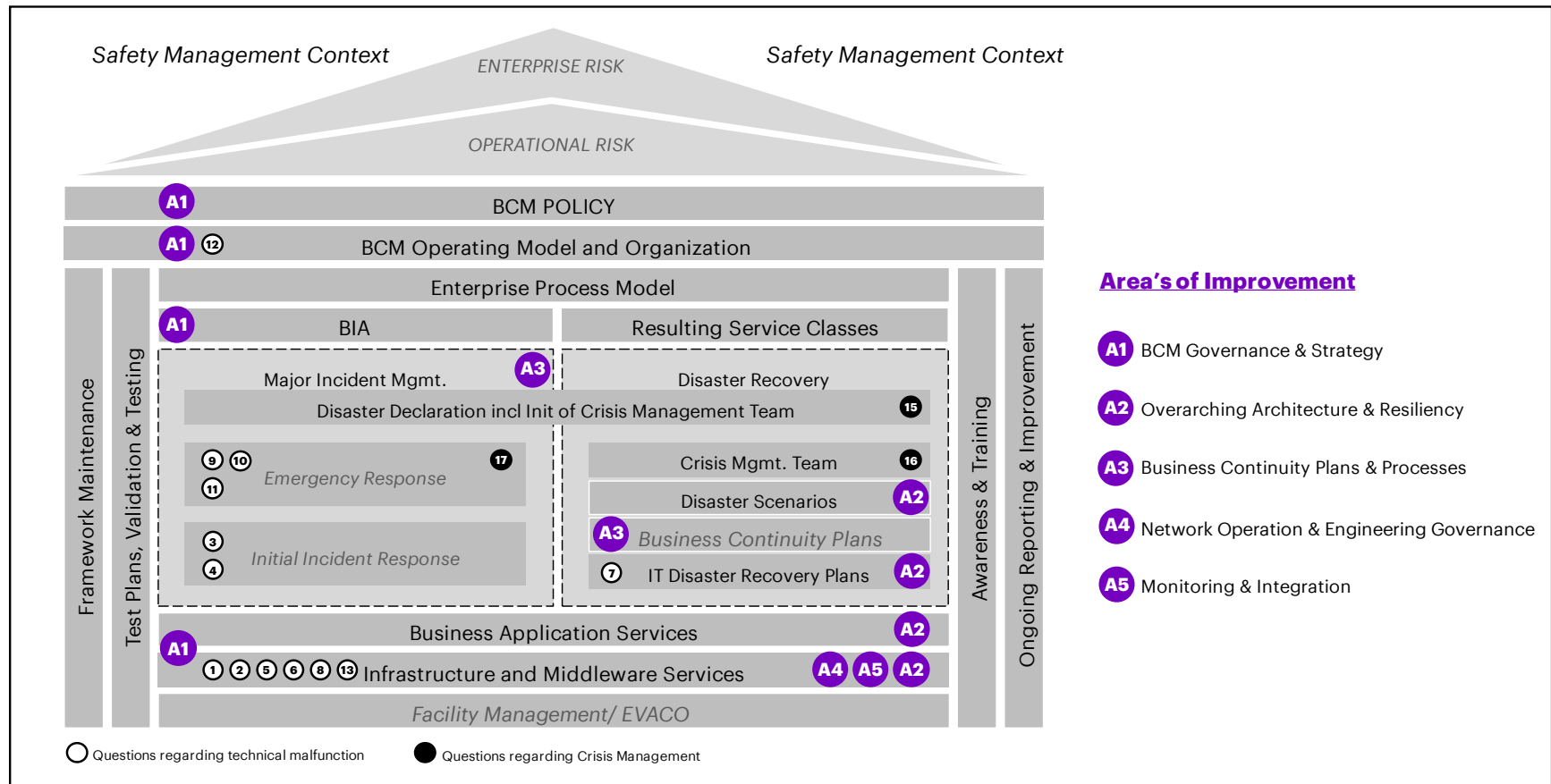


Figure 9: Overview Areas of Improvement for Recommendations



6.1. Prioritization

As per the book of specifications, the recommendations must be prioritized. For this purpose, a priority order will be applied. On top of that, certain levels of estimations are defined in terms of **estimated effort** and **expected added value**:

Effort Level	Estimated Effort	Estimated potential
1	Quick-Win Between 1-3 months	Significant-Added-Value: Significantly improves effectivity and/or efficiency in terms of technology and organizational capabilities
2	Medium-Effort: Between 4-6 months	
3	High Effort: Between 7-12 months	

Table 37: Recommendation - Priority Level Overview

The following table shows an overview of recommendations identified per area of improvement, the applied prioritization and whether the recommendation could be identified on top of the skyguide's internal investigation report:






Area	Nr	Title	Required Effort	New
1	1.1	Refine skyguide's overarching BCM Governance and strategy	2	Yes
	1.2	Improve transparency of skyguide's application and infrastructure	3	Yes
	1.3	Complement existing Business Impact Analysis	1	Yes
2	2.1	Refine and assess skyguide's overarching IT architecture and resiliency	2	No
	2.2	Refine Disaster Recovery strategy	2	Yes
3	3.1	Improve Emergency Checklists applicable for supervisors	2	No
	3.2	Ensure information transparency with ATCOs	1	No
	3.3	Improve communication & collaboration with external stakeholders	1	Yes
4	4.1	Define and Introduce a Network Operation Manual	1	Yes
	4.2	Improve education process for new network technologies	1	No
	4.3	Improve Network Firmware Management Governance	1	Yes
	4.4	Assess depth and breadth of network skills	2	Yes
5	5.1	Define End-to-end Monitoring Strategy	2	No
	5.2	Assess integration of skyguide's future end-to-end monitoring capabilities into COS cockpit	2	Yes

Table 38: Overview Recommendations

As highlighted in the table above, **5 out of 14** recommendations were already mentioned in skyguide's internal report, **9 out of 14** recommendations were identified additionally.

Furthermore, as shown in Figure 10, the recommendations are grouped into two waves and split into a strategic, tactical, and operational level. Recommendations assigned to wave 1 have a strong positive contribution to skyguide's network operation and serve as a baseline for other recommendations. Wave 2 contains recommendations which have a significant dependency on other recommendations and for which skyguide currently has a solution in place with additional room for improvement.



	Wave 1 <ul style="list-style-type: none"> Has strong impacts on skyguide's operations Sets the baseline for other recommendations 	Wave 2 <ul style="list-style-type: none"> Are dependent on other recommendations to be implemented first Skyguide currently has a solution in place but it could be optimized
 Strategical	<div>1.1</div> Refine skyguide's overarching BCM Governance and strategy <div>1.2</div> Improve transparency of skyguide's application and infrastructure <div>5.1</div> Define End-to-end Monitoring Strategy*	<div>2.1</div> Refine and assess skyguide's overarching IT architecture and resiliency* <div>2.2</div> Refine Disaster Recovery strategy
 Tactical	<div>1.3</div> Complement existing Business Impact Analysis <div>4.1</div> Define and Introduce a Network Operation Manual <div>4.3</div> Improve Network Firmware Management Governance <div>4.4</div> Assess depth and breadth of network skills	<div>3.3</div> Improve communication & collaboration with external stakeholders <div>4.2</div> Improve education process for new network technologies* <div>5.2</div> Assess integration of skyguide's future end-to-end monitoring capabilities into COS cockpit
 Operational	<div>3.1</div> Improve Emergency Checklists applicable for supervisors* <div>3.2</div> Ensure information transparency with ATCOs*	

1-3 Months

4-6 Months

7-12 Months

*Already identified in skyguide's internal investigation report

Figure 10: Recommendations in waves

The following chapter provide an overview of recommendations per improvement area.



6.2. BCM Governance & Strategy

Recommendation 1.1: Refine skyguide's Overarching BCM Governance and Strategy	
Description	<p>As part of our investigation, skyguide's current Enterprise Risk Management and Business Continuity Management governance and strategy in the specific context of Safety Management were studied to gain an initial understanding and high-level-overview. Skyguide's BCM is a major part of its Enterprise Risk Management. According to skyguide's definition, its BCM practice consists of three main parts: 1) a Business Impact Analysis (BIA), 2) a business continuity plan and 3) emergency manuals.</p> <p>Our investigation indicates that skyguide defined as part of previous BIA the loss of building A in Dübendorf as considerable disaster event. The loss of building A includes its data center and its Common IFR Room. For this purpose, a first iteration of a disaster recovery plan covering the loss of ANZ-A building was drafted, applicable to the current state of the technical landscape. Skyguide defined as the current state of its technical landscape the landscape as of end Q1 2022. The focus of this disaster recovery plan is on applications used to provision Air Navigation Services.</p> <p>In this scenario, skyguide defined as a disaster recovery plan to build the affected IT landscape from scratch in Geneva including necessary soft- and hardware solutions for the moment. Important to outline is the fact that a minimal service availability requirement applicable for skyguide's IT landscape have not been defined and formally agreed.</p> <p>Taking the above into consideration, our investigation shows that skyguide defined one disaster scenario in a first iterations of disaster recovery checklists, but without a clear association to its critical ANS applications and its underlying technology systems and related sub-components. Furthermore, for each risk and disaster scenario considered as relevant, we recommend defining clear business continuity management objectives in terms of recovery point objective and recovery time objectives,</p>



	<p>also considering and reflecting key guiding principles and requirements.</p> <p>In conclusion, we recommend skyguide to align its overarching BCM governance and strategy with major strategic programs and projects (for example, Virtual Center) moving forward. As a first step, key metrics (Recovery Point Objective, Recovery Time Objective, Service Level Agreements) should be derived from skyguide's overarching safety management and business requirements. This should be considered for all scenario's listed in skyguide's BIA which are relevant for skyguide.</p>
Priority & Justification	<p>2: Estimated Effort between 4-6 months, high potential value-add</p> <p>This recommendation is expected to lay the foundation for skyguide's future IT architecture and related IT program roadmap serving as a foundation for its strategic IT programs.</p>
Relevant findings	8.7.3, 9.1.3

Table 39: Recommendation 1.1 - BCM Governance and Strategy - Overarching BCM Governance and Strategy



Recommendation 1.2 Improve transparency of skyguide's application and infrastructure	
Description	<p>As part of our investigation, information about skyguide's general IT- an BCM setup was requested.</p> <p>Interviews have shown that skyguide does currently lack the understanding of what business processes are supported by which IT infrastructure. Furthermore, it must be noted that skyguide does not have a global view on its application and underlying technology component documentation.</p> <p>Skyguide is actively working on the creation of this mapping. The application view was already built and is available. There is currently no mapping from business process to applications and not from application to the underlying IT infrastructure.</p> <p>The mapping of which business process is operated by which IT infrastructure is helpful to clearly understand what impact a failure of an IT component has on the business and its related applications. If this information is correctly collected, the impact on business could be extracted from the system.</p> <p>We recommend continuing the work on business process to IT infrastructure mapping as this will increase the understanding of an impact in case an IT component failure.</p>
Priority & Justification	<p>3: Estimated Effort between 7-12 months, high potential value-add</p> <p>This recommendation increases the understanding of business process dependencies and lays the baseline to implement recovery time for business processes and services.</p>
Relevant findings	8.1.3, 8.5.1, 8.5.2, 8.10.1, 9.1.1

Table 40: Recommendation 1.2 - BCM Governance and Strategy - Improve transparency of IT landscape



Recommendation 1.3: Complement existing Business Impact Analysis	
Description	<p>As part of our investigation, information about skyguide's general IT- an BCM setup was requested.</p> <p>Our external investigation has shown that various risks were already defined and are reviewed on a regular basis by skyguide. In addition, a work instruction how to create Business Impact Analysis was defined. However, a detailed and extensive Business Impact Analysis which considers the risks resulting from skyguide Enterprise Risk Management practice is not yet available.</p> <p>A Business Impact Analysis is a systematic process to determine and evaluate the potential effects of an interruption to skyguide's critical business services as a result of a disaster. It helps skyguide to adequately design business processes, applications and IT infrastructure and assess IT disaster impacts.</p> <p>We recommend determining and evaluating the potential effects of an interruption to skyguide's critical business services as a result of a disaster (of any type). The already defined risks could be used as an input for the definition of such cases.</p>
Priority & Justification	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>This recommendation increases the understanding of what disasters could happen and what their operational but also financial impact would be.</p>
Relevant findings	9.1.2

Table 41: Recommendation 1.3 - BCM Governance and Strategy - Business Impact Analysis



6.3. Overarching Architecture & Resiliency

Recommendation 2.1: Refine skyguide's overarching IT architecture and resiliency	
Description	<p>One focus of this investigation was to understand various parts of skyguide's overarching IT architecture and resiliency, which was affected by the incident of the 15th of June 2022.</p> <p>Various findings listed in our appendix show that skyguide's architecture design follows a certain set of best practices defined by skyguide's enterprise & system architecture. However, further analysis of skyguide's end-to-end applications and its underlying technology architecture should be conducted. One of our major findings in network architecture was that skyguide has established two independent and redundant networks to fulfill a certain set of resiliency requirements. Skyguide's ANS network is composed of ANS1 and ANS2, two physically independent networks. Applications, affected by the event of the 15th of June 2022 and used to provide ANS-Services, were able to utilize only ANS1 network due to selected design approach at the time of implementation.</p> <p>We recommend assessing the applied architecture principles and implementation of redundancy for applications and its underlying technology components by potentially allowing them to utilize at least two independent physical networks, based on minimal derived key metrics (minimum service availability, recovery point objective, recovery time objective) to be formally defined and aligned with skyguide's key stakeholder DETEC.</p> <p>Taking all this into consideration, we recommend not only applying vendor-specific best practices and principles on specific domains like network (for example, Vlacp, IS-IS, hardware architecture containing redundant Application Specific Integrated Circuits), but also to re-evaluate skyguide's Enterprise & System Architecture principles (Potential end-to-end redundancy capabilities for applications and its underlying technology), reflecting skyguide's safety management and BCM objectives in terms of RTO and RPO.</p>



Priority	2: Estimated Effort between 4-6 months, high potential value-add This recommendation is expected to lay the foundation for skyguide's future IT architecture roadmap and serves as a foundation for its end-to-end-Architecture.
Relevant findings	8.1.1, 8.1.4, 8.1.5, 8.2.1, 8.2.3, 8.2.4, 8.4.2, 9.3.2

Table 42: Recommendation 2.1 - Overarching IT Architecture & Resiliency strategy



Recommendation 2.2: Refine Disaster Recovery Strategy	
Description	<p>From an IT Disaster Recovery point of view, our investigation indicates that skyguide defined as a first iteration of its disaster scenario's the loss of building A and its underlying Common IFR Room and data center. It must also be noted that first disaster recovery plans for this scenario are drafted.</p> <p>However, we recommend not only defining a disaster recovery strategy for only the one scenario already defined within a first iteration (loss of building A), but also for other scenario's resulting from skyguide's Business Impact Analysis (once it can be considered as completed).</p>
Priority & Justification	<p>2: Estimated Effort between 4-6 months, high potential value-add</p> <p>This recommendation helps skyguide to initiate an efficient execution of pre-defined steps on application- and underlying technology layers in case a defined disaster scenario occurs.</p>
Relevant findings	9.2.1

Table 43: Recommendation 2.2 - Overarching IT Architecture & Resiliency - Disaster Recovery Strategy



6.4. Business Continuity Plans, Processes and Checklists

Recommendation 3.1: Improve Emergency Checklists applicable for supervisors

Description

In the event of the 15th of June 2022, BCM plans, processes, and checklists were investigated from a Safety Management point of view. IT Disaster recovery plans and related processes are available only for one certain scenario defined so far which is not applicable in the event of the 15th of June 2022.

From a Safety Management perspective, our investigation indicates that emergency procedures and checklists applicable for a Clear-the-Sky procedure and resume-operation-procedure were applied. The final decision to execute a Clear-the-Sky procedure was taken by the supervisors in Zurich and Geneva. After the Crisis Management Board reported that the technical issue was resolved and stable, the supervisor in Zurich and supervisor in Geneva decided to resume operation.

From a BCM and IT Disaster Recovery point of view, our investigation indicates that skyguide has an overarching Business Continuity Management framework in place which consists of various phases including a comprehensive emergency & crisis management. In the event of the 15th of June 2022, a crisis organization was mobilized according to skyguide's governance. From an organizational point of view, this includes a duty officer, a crisis manager, a chief of staff, a crisis communication cell, a board of crisis management and a supporting group. For each function, skyguide defined the role clearly and the area of responsibilities. The result of our investigation shows that skyguide's overarching crisis- and emergency management governance including policies, processes and checklists were applied effectively with minor exceptions. As outlined in chapter 4, there are some differences between the emergency checklists applicable for ACC Zurich and the checklist applicable for ACC Geneva due to some local characteristics. Furthermore, it must be noted that the checklists did not include the failures of multiple systems at the same time.

In conclusion, we recommend updating the emergency checklists ACC Geneva and ACC Zurich to the most possible extent also considering skyguide's strategic and tactical key



	objectives. Potential harmonization could be considered in case of a companywide operational issue.
Priority	2: Estimated Effort between 4-6 months, high potential value-add Emergency checklists act as a help for the supervisor in critical situation. The purpose of this checklist is to standardize the actions taken in case of an emergency. Outdated or incomplete lists could lead to confusion in emergency situations but also increase the risk of a safety issue.
Relevant findings	9.4.1.1

Table 44: Recommendation 3.1 – Business Continuity Plans, Processes and Checklists – Improve Emergency Checklists



Recommendation 3.2: Ensure information transparency with ATCOs	
Description	<p>As part of this investigation, skyguide's qualitative and quantitative communication analysis were reviewed and additional interviews on this topic were conducted. Additional details can be found in chapter 4.2.</p> <p>In general, it was found, that the internal and external communication was handled as per the process. One finding which was identified in the interviews was that the ATCOs on duty during the day could have been informed more specifically. The ATCOs do not have access to the information shared in the intranet during their shifts and would require an update about the root cause and how it was resolved.</p> <p>A dedicated update for the ATCOs could clarify questions which might be raised after such a technical incident.</p> <p>We recommend providing more information about the technical issue and the status of its current root cause analysis to ATCOs and supervisor's more regularly throughout the crisis management and after the resolution of the issue.</p>
Priority	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>This recommendation targets to resolve potentially raised questions by the ATCOs after a technical issue.</p>
Relevant findings	9.4.2.1

Table 45: Recommendation 3.2 – Business Continuity Plans, Processes and Checklists – Communication ATCOs



Recommendation 3.3: Improve communication & collaboration with external stakeholders	
Description	<p>As part of this investigation, skyguide's qualitative and quantitative communication analysis were reviewed and additional interviews on this topic were conducted. Additional details can be found in chapter 4.2.</p> <p>During our interviews with external stakeholders, it was found that certain groups would suggest changes to the communication as conducted on the 15th of June 2022. During the interview with FOCA, it was stated that one option would be to become part of the COS to receive information in a more efficient way. DETEC GS indicated the desire to be proactively informed in case of major disruptions.</p> <p>Those changes would improve the information flow and allow the groups to take proactive actions in their end.</p> <p>We would recommend considering FOCA in the COS to ensure a more efficient information flow. In addition, DETEC General secretary (GS) and Federal Department of Defense, Civil Protection and Sport (DDPS) and DDPS GS shall directly be informed in case of an emergency or impact of flight operations in the Swiss airspace.</p>
Priority	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>This recommendation targets that information is proactively provided to relevant stakeholders in a most effective and efficient way.</p>
Relevant findings	9.4.3.1, 9.4.3.2

Table 46: Recommendation 3.3 – BCM and DR Plans, Processes and Checklists – Collaboration & Communication with external stakeholders



6.5. Network Operation & Engineering Governance

Recommendation 4.1: Define and Introduce a Network Operation Manual	
Description	<p>As part of this investigation, the network operation governance applied during the event of the 15th of June 2022 was analyzed in chapters 4.5.1 to 4.5.6.</p> <p>One of our major findings is that there is no official network operational handbook in place for Level 2 - Network Operations, which provides clear guidance on how to address network events in an effective and efficient manner.</p> <p>It is recommended to define an operational handbook including a well-defined escalation organization, processes, and responsibilities applicable for Level 2 - Network Operations and Level 3 - Network Engineering.</p>
Priority	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>A proper network operating manual ensures that network events are addressed and troubleshooted effectively and efficiently to ensure a high troubleshooting quality throughout Level 2 - Network Operations.</p>
Relevant findings	8.6.3, 8.8.4, 8.10.4

Table 47: Recommendation 4.1 – Network Operation & Engineering Governance – Network Operation Manual



Recommendation 4.2: Improve education process for new network technologies	
Description	<p>As part of this investigation, the network operation governance applied during the event of the 15th of June 2022 was analyzed in chapters 4.5.1 to 4.5.6.</p> <p>As confirmed during interviews, the Level 2 - Network Operations receives documentation and training from Level 3 - Network Engineering when a new network technology is introduced. The provided information focuses only on the specific new element and does not provide a holistic picture on how it will interact with the remaining network infrastructure landscape.</p> <p>It is recommended to implement training cycles and knowledge exchange forums to further smoothen the processes for introducing new products into skyguide's IT landscape and to ensure common understanding of the internal network architecture landscape.</p>
Priority	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>Improving and leveraging internal knowledge levels within Level 2 - Network Operations will allow for better and quicker maintenance and troubleshooting processes performed by the team.</p>
Relevant findings	8.5.3, 8.5.7

Table 48: Recommendation 4.2 – Network Operation & Engineering Governance – Improve education process



Recommendation 4.3: Improve Network Firmware Management Governance

Description

As part of this investigation, the network operation governance applied during the event of the 15th of June 2022 was analyzed in chapters 4.5.1 to 4.5.6.

Regular alignment: As described in chapter 4.5.1, regular QBR meetings with network switch vendor Extreme Networks and internal alignments are conducted by skyguide. During the meetings discovered bugs applicable for skyguide's environment and new features from which skyguide can potentially benefit are discussed and reviewed. However, results are not documented centrally.

Thus, we recommend to document results discussed during internal and external alignments (meeting minutes).

Firmware evaluation and planning: As stated in chapter 4.5.1, Level 3 – Network Engineering and System Architecture regularly evaluate new firmware release notes and related bug fixes which might be applicable for skyguide's environment. Our investigation indicates that a minimum maintenance release level is regularly discussed during QBR meeting with Extreme Network. However, our investigation has shown that skyguide's firmware evaluation and planning process has only concluded one implementation plan to implement firmware version 8.4.2 (later updated to implement 8.5.1) since 2018. While it is understood that operational stability was a strong factor in maintaining firmware level 7.1.0.0, firmware upgrades should have been implemented as part of the standard release cycle and to avoid creating technological debt.

Furthermore, our investigation has shown that skyguide does not follow formalized firmware evaluation practices to allow a holistic and reasonable set of firmware evaluation and planning principles (such as formal feasibility and risk evaluation of applying certain firmware versions most applicable for skyguide, extent to which vendor recommendations must be applied, exceptions and document formal governance board decisions, etc.).



	<p>Thus, we recommend defining firmware evaluation and planning principles to ensure that certain minimum firmware level recommended by Extreme is applied to skyguide's environment.</p> <p>Firmware testing: Our investigation of skyguide's firmware testing in chapter 4.5.1 has shown that the validation and implementation of firmware upgrades for network devices has taken approximately 12 months to complete for firmware version 7.1.0.0. For firmware version 8.5.1, this time has considerably been reduced to improve efficiency. However, the process and its results are not well documented.</p> <p>Thus, we recommend assessing the process of validating new firmware and hardware releases, reviewing previously identified issues, and running automated tests.</p>
Priority	<p>1: Estimated Effort between 1-3 months, high potential value-add</p> <p>Improving firmware lifecycle management would not only allow skyguide to potentially avoid issues caused by firmware related bugs, but also improve the firmware validation and implementation process efficiency.</p>
Relevant findings	8.5.4, 8.5.6, 8.10.3

Table 49: Recommendation 4.3 – Network Operation & Engineering Governance – Firmware Management



Recommendation 4.4: Assess depth and breadth of network skills	
Description	<p>As part of this investigation, the network operation governance applied during the event of the 15th of June 2022 was analyzed in chapters 4.5.1 to 4.5.6.</p> <p>The total number of switches and related software at skyguide as indicated in the QBR report from 20th of September 2022 was 1129. The recommended number of supported devices is according to general experience approximately 70 per resource.</p> <p>Taking into consideration skyguide's current L2 – Network Operations team size of 15 people, an average of 75,3 network devices is supported by a single resource.</p> <p>We recommend further assessing skyguide's depth and breadth of skills required to effectively and efficiently operate skyguide's network. For this purpose, skyguide's product complexity and product heterogeneity, which was not in scope of this investigation, has to be taken into account.</p>
Priority	<p>2: Estimated Effort between 4-6 months, high potential value-add</p> <p>Sufficient network skills ensure that effective and efficient maintenance and troubleshooting processes can be performed by the L2 – Network Operations.</p>
Relevant findings	8.1.6, 8.5.8, 8.8.2, 8.8.3, 8.9.2

Table 50: Recommendation 4.4 – Network Operation & Engineering Governance – Skill Management



6.6. Monitoring & Integration

Recommendation 5.1: Define End-to-end-Monitoring Strategy	
Description	<p>As part of the investigation, skyguide's monitoring capabilities were also analyzed. Our analysis shows that monitoring solutions used at skyguide consist of various tools in place to provide Level 1 - SMC with a general overview of service status. As part of the incident resolution, iSUP was used by Level 1 - SMC for application monitoring. XIQ and PRTG were used for network management and monitoring by Level 2 - Network Operations and Level 3 - Network Engineering. One of our major findings was that iSUP which is used to monitor end-to-end applications only provides reactive, but not predictive capabilities. The iSUP system can only display the status information of components monitored. Holistic overview cannot be displayed due to the lack data correlation.</p> <p>Automatic Ticket generation: Furthermore, our investigation indicates that current monitoring tools are not configured to automatically generate a ticket when discrepancies in routing of network traffic are detected. We recommend assessing and enabling automated ticket generation capabilities based on certain warning- and error log entries on affected switch devices.</p> <p>Event correlation: In the event of the 15th of June 2022, skyguide's current monitoring systems were not capable of correlating events reported by various devices and predict potential outages of systems and sub-systems. Thus, the initial triage and correlation of events reported to Level 1 - SMC had to be investigated through a time-consuming manual process. We recommend to further assess the monitoring tool capabilities, to use not only reactive but also predictive capabilities based on leveraging historical data of various devices.</p>
Priority	<p>2: Estimated Effort between 4-6 months, high potential value-add</p> <p>Providing accurate, relevant and end-to-end data about application and its underlying technology is crucial for an</p>



	effective and efficient decision making and troubleshooting process.
Relevant findings	8.6.1, 8.6.2, 8.6.4, 8.6.5

Table 51: Recommendation 5.1 – Monitoring & Integration – End-to-end Monitoring



Recommendation 5.2: Assess integration of skyguide’s future end-to-end monitoring capabilities into COS cockpit	
Description	<p>As part of skyguide’s crisis organization, a crisis management and organization cockpit (ECMT) used to govern all crisis processes and related responsibilities in an efficient and centralized way. As indicated during interviews, skyguide’s crisis organization cockpit offers a wide range of capabilities, also including the integration of existing system and monitoring landscape information.</p> <p>Interviews conducted with several stakeholders indicate that essential information collected by several devices are not integrated into skyguide’s crisis organization cockpit. This information had to be collected from different domain-specific teams (application, network, etc) separately which was time-consuming.</p> <p>Taking this into consideration, we recommend integrating key system and sub-system information collected by various devices as well as potential correlation information into skyguide’s crisis management and organization cockpit.</p>
Priority	<p>2: Estimated Effort between 4-6 months, high potential value-add</p> <p>Relevant, clear and holistic information must be provided to relevant COS roles and allows to access the relevant information within one centralized platform. This would allow to assess critical data without connecting to various monitoring tools spread over different environments.</p>
Relevant findings	9.3.1

Table 52: Recommendation 5.2 – Monitoring & Integration – Integration to COS-Cockpit



7. Appraisal of internal investigation report

The objective of this chapter is to appraise the *internal investigation report 2022-06-15 Network Incident* (further named: skyguide's internal investigation report) created by the internal safety investigation team of skyguide, submitted to DETEC at the beginning of October 2022. It must be noted that skyguide's internal investigation focuses on safety management.

In summary, skyguide's investigation report follows a clear structure and provides comprehensible results which can be confirmed for the scope of this investigation (see chapter 1.2). Furthermore, it can be stated that the information provided by skyguide's internal investigation report can in general be considered as complete and correct. However, in some areas the skyguide internal report is incomplete in its findings and could be more stringent in defining recommendations needed. The following chapters provide a summary.

7.1. Communication, Major Decisions, COS

The timeline presented in skyguide's internal investigation report is correct and complete. It was reconstructed listening to the recorded phone calls during the relevant time window, and a summary of relevant phone calls was validated and can be found in the appendix of this present report. Based on interviews it was confirmed that the Clear-the-Sky action was taken in alignment between the supervisor ACC Geneva and the supervisor ACC Zurich. This decision taken was applied to Swiss airspace which corresponds with the skyguide's internal investigation report, resulting in not accepting any further air traffic within the Swiss airspace. The different handling of single flights was confirmed by the supervisor ACC Geneva during an interview. This information is reflected in skyguide's internal investigation report.

Skyguide's internal investigation report shows that the restart of the operations is described from a technical- and from an operational point of view. For both, the technical and the operational point of view, the internal investigation report indicates that COS took the final decision to resume operations. However, this investigation concluded that the ultimate responsibility for the restart of the operation lays with the supervisor ACC responsible for operation. In an interview, it was explained that the COS provides a recommendation to restart operations, but the supervisor ultimately decides. A finding on this topic was defined in skyguide's internal investigation report but was not added to this report as per the reasoning above.

Another important point is that skyguide's internal investigation report lays out, that the emergency checklists were not covering the case of multiple system failures. The emergency checklists were reviewed, and the same conclusion was drawn ending in recommendation 3.1 in Table 44 in this report. The stakeholder communication and COS



meetings are addressed in this present investigation, but not in skyguide's internal investigation report.

Overall, the skyguide's internal investigation report is comprehensive and valid. Certain shortcomings in terms of the COS actions were identified as this topic was only included to a certain extent. Furthermore, several additional internal investigations and lessons learned sessions were conducted by skyguide. Findings of these were not included in the skyguide report:

- External and internal Communication - Technical incident, 15 June 2022
- COS Lessons Learned – System Failure CH & COS Re-Briefing

A brief summary of these two internal investigations is described below:

External and internal Communication - Technical incident, 15 June 2022

A qualitative and quantitative analysis on external and internal communication was conducted by skyguide. In scope of this analysis are the communication provided to skyguide's external key stakeholder groups. Stakeholder communication was only captured briefly in skyguide's internal investigation report. This gap is addressed with this present report. Lessons learned are feasible and valid and do partially align with our findings from the interviews as described in chapter 4.4 (see also chapter 10 – skyguide's information basis, document 2022 10 21 Crisis Communication Incident 15 June 2022 – Accenture.pptx).

COS Lessons Learned – System Failure CH & COS Re-Briefing

As part of the COS process, a final report shall be prepared and stored. A first draft version was shared and addresses, for example, the unavailability of the COS Duty Officer Geneva matching our investigation's findings. In addition, the document stated that a meeting was held with the objective to provide relevant people with an overview lesson learned and resulting changes applied to COS governance (see also chapter 10 - 2022-06-15 COS Event SYSTEM FAILURE CH - Review & Lessons Learned for COS V2022-07-09.pdf).



7.2. Network

In summary, this investigation can confirm that facts stated in skyguide's internal analysis described in chapter 3.6 are generally complete and correct. However, some network related findings and recommendations can be more stringent:

Network Architecture: As described in skyguide's internal investigation report, chapter 3.3.3 Network architecture, the network architecture was designed to be very robust against failure of single elements and failure propagation. However, during this assessment areas of improvement were found and highlighted in chapter 4.5.2 Table 28.

Troubleshooting effectiveness & efficiency: As described in skyguide's chapter "3.1 Network switch failure starting on the 13.06.2022", the monitoring detected an issue on 13th of June 2022 at 14:34. Skyguide's internal investigation report states that the network switch was in a degraded state, nonetheless the incident was closed. The incident from 15th of June 2022 was detected at 01:07 and investigation was started. Facts related to network for the time frame between the 13th and 15th of June can be considered as complete and correct. Skyguide's internal investigation report further states that that skyguide followed their internal escalation process but does not include any statement related to troubleshooting effectiveness and efficiency.

Furthermore, as described in the chapter "3.5.4 Coordination between technicians / engineers of skyguide's internal investigation", the Level 2 - Network Operations and Level 3 - Network Engineering has not been fully prepared to face incidents of such scale. While the internal report indicated that no recommendation was made, this present report has highlighted two recommendations addressing this in chapter 6.5: recommendation 4.1: Define and Introduce a Network Operation Manual and recommendation 4.2: Improve education process for new network technologies. However, this investigation indicates that the first warning message occurred on the 13th of June 2022 was not troubleshooted effectively (see chapter 4.5.1). This present report also derives the necessary recommendations from that situation (see chapter 6).

Network Switch Firmware Management: As described in skyguide's chapter "3.1.2 Upgrade of switches' software (SW) version", skyguide's internal investigation report states that the firmware upgrade requires extensive tests before it can be implemented in production. Still, the time for such evaluation and current test of version 8.5.1 was shortened, compared to the six months test cycle, which was last used in 2018 during 7.1.0.0 implementation.

Furthermore, it is stated in skyguide's internal investigation report that such upgrades have to be managed with caution, as more recent SW versions can improve or correct defects of past versions but can also introduce new ones. However, according to our investigation, the firmware upgrades have not been completed regularly which created



technological debt and related issues (demonstrated by the incident of 15th of June 2022). It must be outlined that maintaining firmware level upgrades is highly recommended to ensure firmware related issues are addressed on time, without negative business impact (see chapter 4.5.6). This present report also derives the necessary recommendations from that situation (see chapter 6).

Usage of skyguide's Network Monitoring Solution: As described in skyguide's chapter "3.1.6 Conclusion concerning the network switch failure analysis", the network architecture and configuration was operating according to the switch vendor's design guidelines from the time when it was deployed. Furthermore, skyguide's internal investigation report states that such a slowly progressing degradation of the internal state of one of the pair of switches is more difficult to detect. However, our investigation indicates that skyguide's network monitoring solution PRTG detected the loss of network traffic on port 1/46 on switch 09 and switch 10 on the 13th of June. This present report also derives the necessary recommendations from that situation (see chapter 6).

On top of the points mentioned above, our investigation can also indicate that recommendations described in skyguide's internal investigation report can be considered as valid. In addition to these recommendations, our investigation provides additional recommendations, as shown in table 38. However, the following restrictions must be taken into consideration:

- Recommendations around application, safety assessment, server and firewall level are not in scope of this investigation and shall be further assessed (R-01, R-08, R-09, R-11, R-12, R-15, R-26).
- Recommendations around Architecture and Governance (R-06, R-07, R-14) can be confirmed, however recommendation R-10 should be further assessed.
- Recommendations around Monitoring (R-02, R-03, R-04, R-05, R-13) can be confirmed, however additional aspects of end-to-end monitoring and COS cockpit integration have been highlighted in chapter 6.6 of this investigation.
- Recommendations around Training (R-23, R-24) can be confirmed, as indicated in recommendation 4.2: Improve education process for new network technologies in Table 48 of this investigation.

Out of scope: Some chapters of the internal investigation could not be verified as they were not in scope of this investigation. This includes ESX VMware, servers, disk storage, TIBCO EMS (Enterprise Message Service), related application behavior, Extreme Networks VSP Defect Tracking Database findings, Extreme Networks tests and verifications, incidents and investigations which occurred on 12th of December 2018, 14th of March 2019, 5th of March 2020, 29th of April 2021, 7th of September 2021, 13th of March 2022.



8. Appendix Network Findings

8.1. Architecture

8.1.1 – Architecture – Usage of independent physical group of network devices for ANS	
Finding	There are two independent and redundant networks: ANS1 and ANS2. Most applications and underlying servers used for ANS are only connected to ANS1 network.
Implication	When one network fails (ANS1) the applications are unable to provide the service through the other network (ANS2)
Recommendation	Assess the implementation of redundancy for applications and its underlying technology components by allowing them to utilize both networks, based on overarching BCM and High-Availability requirements.

Table 53: Network Finding – Architecture - Finding 1 - Usage of independent physical group of network devices for ANS

8.1.2 – Architecture – Redundant power supply	
Finding	A redundant power on a per-cabinet basis in the data center is applied. Two power lines available in the whole room. Devices are connected to both lines. The power supply redundancy is also tested during maintenance activities. Power lines and network cables are secure and separated where possible. The main outlets (used by cleaners etc.) are on a separate power line and are not connected to UPS/generators. There is one source of electricity to the building. It is split into four lines. There are four diesel generators for each main power line and two UPS.
Implication	The power lines and their maintenance are kept up to date, allowing for redundant power supply to the network devices.
Recommendation	Keep.

Table 54: Network Finding – Architecture - Finding 2 - Redundant power supply



8.1.3 – Architecture – Lack of global CMDB documentation	
Finding	There is no global CMDB (Configuration Management Database) documentation in place to effectively track the dependency between skyguide's application and its underlying infrastructure components.
Implication	Lack of one source of information and a complete overview of all resources
Recommendation	Introduction of a CMDB at corporate level and integrating current solutions into one should be further assessed.

Table 55: Network Finding – Architecture - Finding 3 - Lack of global CMDB documentation

8.1.4 – Architecture – Vlacp and IS-IS implementation	
Finding	IS-IS and Vlacp are not implemented on all links
Implication	Lack of link redundancy provided by IS-IS and Vlacp standards.
Recommendation	Assess implementing IS-IS and Vlacp on additional network devices.

Table 56: Network Finding – Architecture - Finding 4 - Vlacp and IS-IS implementation



8.1.5 – Architecture – Switch ASIC architecture	
Finding	Affected network device has only one ASIC chip.
Implication	Failure of such chip can cause an outage of the whole device.
Recommendation	Further assess the possibility of upgrading the network stack with more resilient solutions.

Table 57: Network Finding – Architecture - Finding 5 - Switch ASIC architecture

8.1.6 – Architecture – Availability of Network Architects	
Finding	The number of system and network architects within skyguide is limited.
Implication	There is also a risk of lack of knowledge in a specific area, since there is only one architect. This also reduces role significance causing that architects approval is not mandatory and the architect can be bypassed in the process.
Recommendation	Conduct a skill assessment (depth and breadth assessment of networks skills). Assess the possibility of creating an architecture department.

Table 58: Network Finding – Architecture - Finding 6 - Availability of Network Architects



8.2. Segmentation

8.2.1 – Physical Segmentation – High-Availability Zones	
Finding	No dedicated High-Availability Zones are defined within location Dübendorf. IT Devices are not spread into different High-Availability Zones.
Implication	A minimum of two dedicated high-availability zones within Dübendorf would may improve Skguide’s overall resiliency capabilities
Recommendation	Assess a potential introduction of separate High-Availability-Zones within location Dübendorf based on skyguide’s future BCM Governance and Strategy.

Table 59: Network Finding – Segmentation - Finding 1 - High-Availability Zones

8.2.2 – Segmentation – Vendor lock-in	
Finding	There are more than 1000 devices implemented. Extreme Networks is used for the primary network, Cisco for emergency network, Alcatel for backbone and Nokia for MPLS.
Implication	Different vendors are used to prevent vendor lock in and avoid failure of whole infrastructure due to vendor specific issue.
Recommendation	Keep.

Table 60: Network Finding – Segmentation - Finding 2 - Vendor lock-in



8.2.3 – Segmentation – Physical segmentation	
Finding	Datacenter in Dübendorf is the only Data Center currently being used for certain business critical workloads. Virtual Center project has been launched and is taking into consideration skyguide's future Data Center vision (potentially spread services between multiple data centers).
Implication	Failure of using only one single Data Center in Dübendorf can potentially impact applications and underlying technologies and services (services, network, storage, etc.)
Recommendation	Assess the usage of second Data Center.

Table 61: Network Finding – Segmentation - Finding 3 - Physical segmentation

8.2.4 – Segmentation – Office network redundancy	
Finding	Office network is separated. Office network has no redundancy.
Implication	Office network has no impact on the crucial network components.
Recommendation	Assess the possibility of introducing redundancy to avoid network failures during network maintenance.

Table 62: Network Finding – Segmentation - Finding 4 - Office network redundancy



8.3. Product Life Cycle Management

8.3.1 – Product Life Cycle Management – Product validation	
Finding	Skyguide has a process for validating new software and hardware. There is a separate network where changes can be validated and tested.
Implication	New features can be tested in a dedicated, isolated network before rolling-out into production environment without affecting productive load.
Recommendation	Keep

Table 63: Network Finding – Product Life Cycle Management - Finding 1 - Product validation

8.3.2 – Product Life Cycle Management – Relationship with vendors	
Finding	Skyguide has a good relationship and a closed exchange with the vendors. Quarterly Business Review meetings are taking place.
Implication	Fast vendor support and get an early information about new product, releases and features.
Recommendation	Keep.

Table 64: Network Finding – Product Life Cycle Management - Finding 2 - Relationship with vendors



8.3.3 – Product Life Cycle Management – Regular checks of EoL and EoS	
Finding	Skyguide evaluates on a regular basis End of Support, End of Life and End of Sales dates with vendors.
Implication	To ensure that life cycle projects are triggered on the right time.
Recommendation	Keep.

Table 65: Network Finding – Product Life Cycle Management - Finding 3 - Regular checks of EoL and EoS

8.4. Security

8.4.1 – Security – Data Center audits	
Finding	Data Center audits are performed once a year by network technicians coming from airports in other countries.
Implication	Audit is completed by engineers from airports in different countries and not by an independent external party.
Recommendation	Assess implementation of 3 rd party external audits to ensure that standards and best practices are always up to date.

Table 66: Network Finding – Security - Finding 1 – Data Center audits



8.4.2 – Security – Permissions	
Finding	Entrance to the technical room where servers are operating is restricted. Personnel needs to have correct permissions assigned to their badge and as a second layer of authentication they need to provide a PIN to enter the room. Cabinets are not individually locked. Cabinets are not monitored by monitoring cameras.
Implication	All network equipment and servers are stored in one big area. Entering the area gives access to all cabinets. There is no logbook to confirm who was performing what actions.
Recommendation	Assess the possibility of moving or splitting the area into smaller parts would help increase physical security and ensure that minimum access is granted.

Table 67: Network Finding – Security - Finding 2 - Permissions



8.5. Continuous Service Improvement

8.5.1 – Continuous Service Improvement – Network documentation and diagrams	
Finding	Documentation and diagrams are not being kept up to date. Documentation and diagrams have outdated information, such as port numbers and device locations.
Implication	This adds complexity for management and troubleshooting.
Recommendation	Assess the possibility of creating centralized document or a system with up-to-date information as a central source of information. The central source can be linked in all other documents, allowing for quick and easy management and full overview of all connected devices on physical and logical layer.

Table 68: Network Finding – Continuous Service Improvement - Finding 1 - Network Documentation and Diagrams

8.5.2 – Continuous Service Improvement – General Data Center layout	
Finding	Data Center room is well managed and maintained. The equipment is well organized. Cabling inside the Data Center is very well maintained, including the layout and labeling. Some racks have layout documentation available directly on the rack to allow better and more efficient maintenance. There is no Floor Plan with rack location and zone description located at the entrance.
Implication	Simplifying the installation processes of maintenance components and troubleshooting.
Recommendation	Assess adding Floor Plan with rack location and zone description located at the Data Center entrance.

Table 69: Network Finding – Continuous Service Improvement - Finding 2 - General Data Center layout



8.5.3 – Continuous Service Improvement – Knowledge transfer	
Finding	Knowledge management governance has been implemented at skyguide. Documentation is maintained and new documentation is created and provided to Network Operations when new network technology is implemented. Having correct and up to date documentation is a part of the implementation project. Network Operations are trained on the new technology and processes. The process ensures quality of the training, which must be confirmed during handover. The information provided to Network Operations focuses only on the new system/process which is being implemented and does not provide overall understanding of the networking landscape. Time required to familiarize with the new information is not guaranteed. Information about the overarching network landscape can be time consuming to obtain, which has direct impact on investigation time.
Implication	Knowledge transfer process has been implemented. However, the process does not guarantee holistic understanding of the network environment which is required for effective troubleshooting.
Recommendation	Assess how knowledge transfer can be further improved on a regular basis.

Table 70: Network Finding – Continuous Service Improvement - Finding 3 - Knowledge transfer



8.5.4 – Continuous Service Improvement – Firmware management governance	
Finding	The process of implementing firmware was not completed on a regular basis. The selected approach to apply firmware releases is considered to be very safety driven and reactive. This has resulted in skyguide not having firmware implementations since November 2018, omitting opportunities to upgrade firmware over the course of the past four years.
Implication	Latest features and bug fixes are not available. Selected implementation approach has caused additional delays due to additional requirements, such as firmware minimum level on new hardware.
Recommendation	Assess internal processes to find possible improvements. Increase efficiency of implementing software fixes released by the vendors.

Table 71: Network Finding – Continuous Service Improvement - Finding 4 - Firmware management governance

8.5.5 – Continuous Service Improvement – Regular power supply maintenance	
Finding	During yearly maintenance actions on network devices redundant power supply is tested. Power generators are also tested every 6 months.
Implication	Power supply delivery is well maintained and tested.
Recommendation	Keep.

Table 72: Network Finding – Continuous Service Improvement - Finding 5 - Regular power supply maintenance



8.5.6 – Continuous Service Improvement – Firmware upgrade process	
Finding	The efficiency of skyguide’s firmware upgrade cycle was improved, when skyguide started to evaluate firmware version 8.5.1. The process consists of documentation analysis, assessment and testing of actual firmware in two separate test environments, and implementation to the production environment. The process is not well documented.
Implication	The validation and implementation processes have been recently improved. However, this could have been one of the factors preventing skyguide from implementing current firmware levels. Being able to implement critical software fixes quickly is crucial for successful operation.
Recommendation	Further assess how validation process can be improved to reduce the required numbers of tests, automation and efficiency. Further assess the configuration of production network environment to be able to utilize its redundancy for an effective and no disruption implementation cycle.

Table 73: Network Finding – Continuous Service Improvement - Finding 6 - Firmware upgrade process



8.5.7 – Continuous Service Improvement – Regular audits	
Finding	Yearly audits are performed by personnel coming from other airports. This is an assessment only. Best practices or other suggestions are not discussed. There is no knowledge exchange group created between the airports.
Implication	Audits are performed internally by airports network operators and not by 3 rd party. Audits do not include knowledge and best practices exchange.
Recommendation	Assess completing audits by an independent 3 rd party and implementing knowledge exchange cycles for the airport network operators.

Table 74: Network Finding – Continuous Service Improvement - Finding 7 - Regular audits

8.5.8 – Continuous Service Improvement – Process standardization	
Finding	Not all processes (e.g. Handover to Operations) which were implemented recently are following the formal processes.
Implication	Processes are becoming less standardized.
Recommendation	Assess and update the formal processes. Assess human resources requirements to ensure processes can be adhered to on a daily basis.

Table 75: Network Finding – Continuous Service Improvement - Finding 8 - Process standardization



8.5.9 – Continuous Service Improvement – Independent fire extinguishing system	
Finding	Each cabinet has its own independent fire extinguishing system, allowing to extinguish the fire directly in the cabinet without affecting other cabinets. Lifted floors protect electrical equipment from water damage. The Data Center room provides adequate free space to allow easy movement, helping to avoid accidents.
Implication	The fire and water hazard safety precautions are implemented according to industry best practices.
Recommendation	Keep.

Table 76: Network Finding – Continuous Service Improvement - Finding 9 - Independent fire extinguishing system

8.6. Monitoring

8.6.1 – Monitoring – No holistic end-to-end-monitoring capabilities in place	
Finding	iSUP is currently not capable of providing holistic and historical information-based data points provided by skyguide's managed devices.
Implication	Events captured by iSUP are not correlated to other events. Thus, it is time consuming for Level 1 - SMC to initially triage and isolate the problem.
Recommendation	Conduct a further assessment of not only reactive, but also predictive monitoring capabilities offering end-to-end data flows of end-to-end applications and underlying technology stack being used.



Table 77: Network Finding – Monitoring - Finding 1 - No holistic end-to-end-monitoring capabilities in place

8.6.2 – Monitoring – Monitoring as an integral change and request process part	
Finding	Monitoring component is not a part of skyguide’s request and change management process at the very beginning.
Implication	Implementation time of monitoring capabilities and quality can be impacted.
Recommendation	Monitoring to be considered as a major part of skyguide’s request and change management process at the very beginning.

Table 78: Network Finding – Monitoring - Finding 2 - Monitoring as an integral change and request process part

8.6.3 – Monitoring – Troubleshooting and investigation process	
Finding	Investigation of the incident which occurred on the 13 th of June 2022 was only investigated on a port level, but not on Vlapc level.
Implication	Investigation on a Vlapc link level may have led to further analysis and issue resolution.
Recommendation	Assess skyguide’s network operation manuals and principals to ensure holistic troubleshooting approaches and right utilization of skyguide’s tools capabilities.

Table 79: Network Finding – Monitoring - Finding 3 - Troubleshooting and investigation process



8.6.4 – Monitoring – Configuration of network monitoring tools	
Finding	XIQ monitoring tool provided by Extreme networks has certain limitations. The tool automatically discovers and links only devices produced by Avaya and Extreme Networks. As skyguide uses also devices produced by other manufacturers, such devices must be added manually and all links between devices also need to be created manually. For such devices XIQ does not provide complete support functionality which introduces further limitations.
Implication	This may create differences as manual process does not follow a common standard. This allows different naming conventions to be applied and raises the risk that links will be correctly created and updated over time. Additionally, the support complexity increases as not all functions are available to Level 2 - Network Operations and Level 3 - Network Engineering for all devices.
Recommendation	Assess network monitoring capabilities and architecture. Assess implementation of new monitoring tools which integrate fully with skyguide's IT architecture.

Table 80: Network Finding – Monitoring - Finding 4 - Configuration of network monitoring tools



8.6.5 – Monitoring – Configuration of alerts in the monitoring tools	
Finding	Information available to Level 1 - SMC and Level 2 - Network Operations can be displayed differently, due to differences in configuration between monitoring tools. Some of the systems are providing monitoring data directly to Level 1 - SMC and XIQ, while others are providing data only to XIQ which is then transmitting the information to Level 1 - SMC. Differences in interpretation of data between XIQ and Level 1 - SMC depend on the monitoring alarm configuration in both systems.
Implication	Monitoring tools are not aligned and displayed information can differ when compared between the tools.
Recommendation	Ensure that created alerts and data processing follows a standardized and well documented process. Assess data processing automation through centralized tools.

Table 81: Network Finding – Monitoring - Finding 5 - Configuration of alerts in the monitoring tools



8.7. Isolation and Failover Tests

8.7.1 – Isolation and Failover Tests – Power redundancy	
Finding	Servers and network devices are connected to two power lines. During each maintenance activity, power redundancy is tested.
Implication	Power redundancy is evaluated by conducting regular tests.
Recommendation	Keep.

Table 82: Network Finding – Isolation and Failover Test - Finding 1 - Power redundancy

8.7.2 – Isolation and Failover tests – Validation of power redundancy	
Finding	Skyguide has completed an entire datacenter shutdown by cutting down all power lines to the data center. This test was performed in 2007/2008 to ensure all equipment is functioning as required.
Implication	Skyguide verified that its power redundancy concept functions as expected.
Recommendation	Keep.

Table 83: Network Finding – Isolation and Failover Test - Finding 2 - Validation of power redundancy



8.7.3 – Isolation and Failover tests – IT SLA	
Finding	Our observations indicate a lack in definition of the business continuity & disaster recovery requirements (in terms of Recovery Point Objective and Recovery Time Objective) to IT Service Level Agreements (IT SLAs). Furthermore, a lack of a BCM (Business Continuity Management) and DR (Disaster Recovery) plan was observed, that specifies which hazards IT services must sustain.
Implication	With SLA in place, IT has clear specifications on how to build services and redundancies to meet or exceed the SLA's. Whether the built-in redundancy is sufficient for the business, can only be confirmed if SLA's and BCM/DR plans are in place.
Recommendation	Assess business continuity & disaster recovery requirements, ensure alignment with IT Service Level Agreements and establishment of Business Continuity Management and Disaster Recovery plans.

Table 84: Network Finding – Isolation and Failover Test - Finding 3 - IT SLA



8.8. End-to-end Service Fulfillment

8.8.1 – End-to-end Service Fulfillment – Quality Management of new platforms	
Finding	Process and Quality Management is in place between Engineering and Operation when introducing new platforms.
Implication	Implemented processes allow to implement high quality platforms.
Recommendation	Keep.

Table 85: Network Finding – End-to-end Service Fulfillment - Finding 1 - Quality Management of new platforms

8.8.2 – End-to-end Service Fulfillment – Network as a single service	
Finding	Network is considered as a single service.
Implication	From service point of view network is managed as a single construct.
Recommendation	Further assess how responsibilities for each network area are split between support teams to assure correct coverage and skillset availability.

Table 86: Network Finding – End-to-end Service Fulfillment - Finding 2 - Network as a single service



8.8.3 – End-to-end Service Fulfillment – Skillset and certification	
Finding	Resolution of a network related incident follows an escalation path. The escalation path has been defined; however, the skillset and certification level vary.
Implication	When service disruption is discovered support personnel can escalate the issue to the next level of support. Support personnel does not have a well-defined certification and upskilling path.
Recommendation	Assess training possibilities, inhouse upskilling by knowledge sharing sessions and job shadowing.

Table 87: Network Finding – End-to-end Service Fulfillment - Finding 3 - Skillset and certification

8.8.4 – End-to-end Service Fulfillment – Resource availability	
Finding	Level 3 - Network Engineering is not obligated to be involved in a formal escalation process. As stated by Level 2 - Network Operations, there is only a so-called informal agreement in place between Level 2 - Network Operations and Level 3 - Network Engineering.
Implication	Level 3 - Network Engineering is not required to provide support outside of standard business hours. This may result in delayed resolution of complex network incidents.
Recommendation	Refine skyguide's on-call duty governance also considering Level 3 - Network Engineering.

Table 88: Network Finding – End-to-end Service Fulfillment - Finding 4 - Resource availability



8.9. Employee Training Concept

8.9.1 – Employee Training Concept – Internal training	
Finding	The network operation team is involved in the training events, which are organized by the network engineering team.
Implication	The network operation team received hands-on experience and documentation materials.
Recommendation	Keep.

Table 89: Network Finding – Employee Training Concept - Finding 1 – Internal training



8.9.2 – Employee Training Concept – Training effectiveness	
Finding	<p>The investigation of the incidents which are in scope of this investigation were not performed to the best practices. For example:</p> <ul style="list-style-type: none">- Investigation was performed only on one switch even though the second switch was reporting an issue on the 13th of June 2022.- On 13th and 14th of June 2022 no troubleshooting or investigation actions were performed on switch 09.- 38 hours and 20 minutes spent before switch 09 was rebooted since the initial problem was reported.
Implication	Delayed problem resolution.
Recommendation	Create network operating manuals to ensure that network events are addressed and troubleshooted effectively and efficiently. Assess training possibilities, inhouse upskilling by knowledge sharing sessions and job shadowing.

Table 90: Network Finding – Employee Training Concept - Finding 2 - Training effectiveness



8.10. Change Management

8.10.1 – Change Management – Update documentation when conducting a change	
Finding	Position of the switch 09 and switch 10 is correct in Racks B21 and B10 as per documentation. Some devices in the rack are different than devices listed in the documentation.
Implication	Physical location of the devices can change over time. When such change occurs not all documents containing location information are updated on a timely manner, causing delays for support personnel to locate the device in the server room.
Recommendation	To avoid such risks, a central document or an interactive system should be implemented, where up to date information for all racks can be stored. Other documentation and manuals should have references to this document/system.

Table 91: Network Finding – Change Management - Finding 1 - Update documentation when conducting a change

8.10.2 – Change Management – Change management process	
Finding	Changes which are implemented to the network environment are listed in the QBR report and discussed. Changes follow approval process. This includes network switch firmware upgrades.
Implication	Each change follows review and approval processes and are documented.
Recommendation	Keep.

Table 92: Network Finding – Change Management - Finding 2 - Change management process



8.10.3 – Change Management – Firmware management	
Finding	Network switch firmware testing and approval database is not kept up to date. Documentation of completed firmware evaluations is not available.
Implication	Lack of current documentation on evaluated, tested and approved firmware levels.
Recommendation	Adhere to the process of continuous documentation actualization.

Table 93: Network Finding – Change Management - Finding 3 - Firmware management

8.10.4 – Change Management – Escalation processes	
Finding	The network switch vendor Extreme Networks has recommended network switch replacement. This task was completed by skyguide, however, as of the time of writing this report, Extreme Networks has not contacted skyguide after receiving the network switch for further analysis.
Implication	Skyguide does not have effective follow-up and escalation processes to ensure successful task completion. Investigation of the failed network switch has been ongoing since 15 th of June 2022.
Recommendation	Assess vendor management area and ensure that projects and tasks are managed in a way to provide successful task completion.

Table 94: Network Finding – Change Management - Finding 4 - Escalation processes



9. Appendix Crisis Management Findings

9.1. Business Continuity Management

9.1.1 – Business Continuity Management – Holistic Mapping of Business Processes to IT	
Finding	Lack of holistic understanding of business impact in case of application or IT infrastructure failure
Implication	In case of an application or underlying IT component failure, impact on the related business processes is not clearly understood.
Recommendation	Create a holistic view which shows the mapping of skyguide's business process to its associated application- and IT infrastructure components and reflect results in skyguide's CMDBs.

Table 95: Crisis Management Findings – Business Continuity Management - Finding 1 - Holistic Mapping of Business Processes to IT

9.1.2 – Business Continuity Management – Full Business Impact Analysis	
Finding	A policy on how to create Business Impact Analysis is available but there was no holistic impact analysis conducted for various disaster scenarios
Implication	Even though the ATM is safety driven, impacts of IT disasters are not fully defined and the financial, reputational and customer impacts are not fully understood.
Recommendation	Complement skyguide's Business Impact Analysis also considering risks identified as part of skyguide's enterprise risk assessment.

Table 96: Crisis Management Findings – Business Continuity Management - Finding 2 - Full Business Impact Analysis



9.1.3 – Business Continuity Management – Lack of BCM objectives	
Finding	Business continuity objectives in terms of RPO and RTO are not defined.
Implication	Skyguide's current IT architecture is based on internally defined BCM objectives.
Recommendation	Define and align BCM objectives with skyguide's key stakeholders

Table 97: Crisis Management Findings – Business Continuity Management - Finding 3 - Lack of BCM objectives

9.2. Disaster Recovery

9.2.1 – Disaster Recovery – Disaster Recovery Plans and Cases	
Finding	Lack of IT disaster recovery plan and disaster scenarios.
Implication	No specific guideline available on how to recover applications and underlying infrastructure components in case of a disaster.
Recommendation	Complement disaster recovery plans and define further cases.

Table 98: Crisis Management Findings – Disaster Recovery - Finding 1 - Disaster Recovery Plans and Cases



9.3. Crisis Management

9.3.1 – Crisis Management – System status for COS	
Finding	Various information had to be obtained by COS, including but not limited to system status information provided by Level 1 – SMC.
Implication	Information gathering for various sources was time consuming.
Recommendation	Integrating key system and sub-system information to the COS.

Table 99: Crisis Management Findings – Crisis Management - Finding 1 - System status for COS

9.3.2 – Crisis Management – NOTAM Tool Availability	
Finding	The tool to publish NOTAMs (SCONE) was impacted by the system disruption.
Implication	The contingency plan was executed as per work instructions.
Recommendation	Increase system resiliency for systems used by AIM.

Table 100: Crisis Management Findings – Crisis Management - Finding 2 - NOTAM Tool Availability



9.3.3 – Crisis Management – Access Control to Common IFR Room (CIR)	
Finding	Roles of certain people physically present in the Common IFR Room in Geneva were unclear for the supervisor.
Implication	Caused confusion/distraction for the supervisor.
Recommendation	Clarify roles of people physically present in the Common IFR Room in Geneva in case of a crisis.

Table 101: Crisis Management Findings - Crisis Management - Finding 3 - Access Control to Common IFR Room (CIR)

9.3.4 – Crisis Management – Sharing Lessons Learned with Supervisors	
Finding	Exchange lesson's learned within supervisor groups located in Zurich and Geneva only present to a minimum extent.
Implication	Other/newer supervisors do not take benefit from lesson's learned.
Recommendation	Conduct regular knowledge sharing sessions between supervisor groups.

Table 102: Crisis Management Findings – Crisis Management - Finding 4 - Sharing Lessons Learned with Supervisors



9.4. Detailed background and dedicated questions

9.4.1. Adhering to COS Process

9.4.1.1 – Adhering to COS Process – Emergency Checklist Update	
Finding	Emergency checklist do not cover failure of multiple applications and/or underlying technology components.
Implication	In case of certain incidents, the supervisor does not have the required guideline to act accordingly.
Recommendation	Update emergency checklists to cover cases aligned with the new IT design considering dependencies and impacts of IT infrastructure and system failure.

Table 103: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 1 - Emergency Checklist Update

9.4.1.2 – Adhering to COS Process – Availability of Duty Officer	
Finding	The COS Duty Officer Geneva was not reachable during the escalation.
Implication	COS Duty Officer in Zurich was notified. This could have led to a certain delay in escalation but did not majorly impact the escalation.
Recommendation	Ensure availability of COS Duty Officer.

Table 104: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 2 - Availability of Duty Officer



9.4.1.3 – Adhering to COS Process – Information sharing during escalation	
Finding	During the briefing of the COS Duty Officer Zurich, it was unclear that the technical issue concerned both locations.
Implication	It took a certain amount of time for the COS Duty Officer Zurich to understand the impact of the technical malfunction and to realize that both locations are affected.
Recommendation	Ensure consistent and relevant information sharing during escalation process by applying standard question list.

Table 105: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 3 - Information sharing during escalation

9.4.1.4 – Adhering to COS Process – Reduced Participants at COS Orientation Report	
Finding	The COS Orientation report was only held in Zurich.
Implication	People who were already in the COS room in Geneva were informed about the situation at a later stage.
Recommendation	Ensure execution of checklist “Commissioning of the crisis rooms” by increasing the awareness.

Table 106: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 4 - Reduced Participants at COS Orientation Report



9.4.1.5 – Adhering to COS Process – Individual flight handling	
Finding	Individual flights were handled differently after the decision was taken to Clear-the-Sky: While ACC Zurich accepted only certain single planes, ACC Geneva did not further allow any planes at all.
Implication	Uncertainty for the supervisors on how to cope with the situation.
Recommendation	Clarify and define if actions should be fully aligned between ACC Zurich and ACC Geneva in case of a skyguide wide service disruption.

Table 107: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 5 - Individual flight handling

9.4.1.6 – Adhering to COS Process – Minimal IT Service Definition	
Finding	Within skyguide, there is no common understanding or definition about minimal IT technical services.
Implication	Lack of common understanding of what minimal IT services are required to fulfill skyguide's minimal operational objectives.
Recommendation	Provide a formal definition of skyguide's minimal IT services required to provide ATM functions to ensure a common understanding

Table 108: Crisis Management Findings – Detailed background and dedicated questions – Adhering to COS Process – Finding 6 - Minimal Service Definition



9.4.2. Communication, Collaboration and decision-making process

9.4.2.1 – Communication – Information sharing with important stakeholders	
Finding	Important individuals could have been informed more frequent: <ul style="list-style-type: none">• ATCOs• Reception
Implication	When the work was resumed, no information/update on the root cause of the technical malfunction was provided to the ATCOs. In addition, the reception was not provided with a dedicated update or instructions who to grant access to.
Recommendation	Provide ATCOs with relevant information before ATCOs continue with operational responsibilities. In addition, update the reception on expected visitors and prepare them in case journalists will arrive.

Table 109: Crisis Management Findings – Communication - Finding 1 - Information sharing with important stakeholders

9.4.2.2 – Communication – Media Publications using Meltwater Platform	
Finding	Meltwater was unable to support the amount of media releases that were supposed to be published.
Implication	The contingency procedure for media releases (email) was executed.
Recommendation	Increase the amount of media releases possible to publish using the Meltwater platform.

Table 110: Crisis Management Findings – Communication - Finding 2 - Media Publications using Meltwater Platform



9.4.3. Stakeholder opinions on communication

9.4.3.1 – Stakeholder opinions on communication – Including FOCA into COS	
Finding	FOCA was informed but expressed their desire to be included in the COS.
Implication	Information flows were indirect.
Recommendation	Include FOCA in the COS.

Table 111: Crisis Management Findings – Stakeholder opinions - Finding 1 - Including FOCA into COS

9.4.3.2 – Stakeholder opinions on communication – Directly informing DETEC	
Finding	DETEC GS was not informed immediately after the incident was detected by skyguide
Implication	Proactive measures could only be implemented by DETEC with a delay.
Recommendation	Inform DETEC GS and DDPS GS in case of major incidents in air traffic immediately after such an incident occurred.

Table 112: Crisis Management Findings – Stakeholder opinions - Finding 2 - Directly informing DETEC



10. Appendix Information Basis

Requested document	Received document
IT Organigram	Organigram T-TP-TM 2022.xlsx Skyguide org chart extract.pptx
Description of network department incl. approved MAK / currently occupied roles	OneNote document: Occupied Role Open Notebook.onetoc2 Section sans titre.one Skyguide org chart extract.pptx
Business Organization handbook /Manual	C2WI8011E_NELCH_(Innovation_&_Change_Management_-_Network_Services).pdf Enterprise Application Landscape Diagram.svg ISUP - Application Interface - MV-NT Diagram.svg ISUP Application Context View Diagram.svg EA scope.jpg
Roles and Process Description	C3WI8400E - SMS Procedure.pdf
Products and Software Portfolio and Roadmap	Extreme roadmap.docx Skyguide QBR 2022-OC2FO8102E - Test Plan - Release 8.5.1.0.docm C2FO8103E - Test Protocol - New Release upgrade 8.5.1.0.pdf C2FO8103E - Test Protocol - Release upgrade 8.5.1.0 – Rollback.pdf C2FO8103E - Test Protocol - Release upgrade 8.5.1.0.pdf C2FO8103E - Test Protocol - Release_Compatibility_8.5.1.0.pdf C2FO8103E - Test Protocol - Release_Monitoring_8.5.1.0.pdf9-20.pdf
CMDB including installed, products, model, vendor, current software version, number of operated network devices.	VSP+ ERS-XIQ_ANS_101322134902.xlsx



Design Guidelines with Building Blocks including SLAs per Building Block	AVAYA_Campus_LAN_Reference_Design.pdf
	AVAYA_Data_Center_Reference_Design.pdf
	NN48500-649_Network_Virtualization_using_Extreme_Fabric_Connect.pdf
SLA Documents, service Portfolio	Configuring the SLA Mon Agent
Standard configuration and Network Plans	Implementation and Configuration Guide Avaya VSP_v7.1.pdf
	Documentation Reference for VSP Operating System Software VOSS 7.1 Configuration Guides
	Quick Start Configuration for VSP Operating System Software
	Using CLI and EDM on VSP Operating System Software
	Command Line Interface Commands Reference
	Configuring VLANs, Spanning Tree, and NLB on VSP Operating System Software
	Configuring QoS and ACL-Based Traffic Filtering on VSP Operating System Software
	Configuring Link Aggregation, MLT, SMLT and vIST on VSP Operating System Software
	Configuring IP Multicast Routing Protocols on VSP Operating System Software
	Configuring IPv4 Routing on VSP Operating System Software
	Configuring OSPF and RIP on VSP Operating System Software
	Configuring IPv6 Routing on VSP Operating System Software
	Backbone Network Architectural Design.pdf
	General Architecture.docm.pdf
	MICS Implementation and Configuration Guide - Avaya Stackable Switches.pdf



	Network Architecture and Detailed Configuration IPSERV RFC2033m.pdf
	Network Architecture and Detailed Configuration VIS@S 2295.pdf
	Network details Subnet and ports.xlsx
	virtual networking configuration.docm
	Route check list.xlsx
	Screenplay Vis@s ODD.xlsx
	Test_Protocol_Visas_ODD.docm
	Visas ODD PWAE_Request.docx
	VLAN Inventory ODD Visas ANS.xlsx
	Configuring BGP Services on VSP Operating System Software
	Configuring Fabric Basics and Layer 2 Services on VSP Operating System Software
	Configuring Fabric Multicast Services on VSP Operating System Software
	Administering VSP Operating System Software
	Configuring Security on VSP Operating System Software
	Troubleshooting VSP Operating System Software
	Monitoring Performance on VSP Operating System Software
	Configuring Fabric Layer 3 Services on VSP Operating System Software
	Configuring VXLAN Gateway on VSP Operating System Software
	VSP Operating System Software Alarms (sorted by ID)
Service and Maintenance processes and contracts	19.06.25 - 959321_20190621_bnc_offer_maintenance_extreme_v02e.pdf
	List of interventions on Swiches 009 - 010 - 001 and 002: DUBV72A1A009.xlsx DUBV72A1A010.xlsx DUBV82A1A001.xlsx DUBV82A1A002.xlsx
	C3MA8001E Manual for ATM AIM Technical Services.pdf



	C3PD8000E Technical Service Delivery.pdf
	C3WI8020D Organisation des Garantierten Interventionsdienstes (GID).pdf
	C3WI8030E WAC.pdf
	DR0001E-A01_skyguide_Process_Landscape.pdf
Description of network, security, and performance monitoring solutions	NMS replacement-SMC requirement draft march 2020.docx
	PRTG Confluence.url
	XIQ Confluence.url
	XMC Connections Design.vsdX
	XMC Failure workflow.vsdX
	XMC Network Architecture and Detailed Configuration.docm
	XMC Operating Organization.docm
	XMC setup for SMC and ISUP integration.pdf
	XMC setup for SMC,ISUP integration.vsdX
All relevant information related to Clear-the-Sky-event: including but not limited to timing of the fault up to the point at which it is rectified, logs, network documentation of affected switched cluster	Business capabilities and data flows.pptx
	June 15th 2022 Log OPS extracts SPVR ACC.pptx
	DUBV82A1A001_log.49300001.123
	DUBV82A1A001_log.49300001.124
	DUBV82A1A001_log.49300001.125
	DUBV82A1A002_log.49480001.124
	DUBV82A1A002_log.49480001.125
	DUBV82A1A002_log.49480001.126
	DUBV82A1A002_log.49480001.127
	DUBV82A1A002_log.49480001.128
	fulltech_DUBV82A1A001.txt
	fulltech_DUBV82A1A002.txt



	15.06.2022 Incident Task Force Status Meeting Protocols
	URGENT _ Explanation of the technical failure of the 16th - A first immediate mandate.msg
	20220615-103805_log.pdf
	20220615-104656_log.pdf
	ECMT protocols export.pdf
	ECMT tasks export.pdf
	01 – History.pdf
	02 - Baseline Situation.pdf
	03 - Log Files - Status data.pdf
	04 - RCA Reports.pdf
	10 - Upgrade Plan.pdf
	RCA 15.06.2022 Incident.pdf
	Ticket GVA InspectorConsole I220615_0003 anonymized.pdf
	Ticket ZRH InspectorConsole I220615_0001 anonymized.pdf
	Switches 009 & 010 backup files
	Switches 009 & 010 FullTech before reboot (dump file)
	Switches logs from 13.06 to 16.06
	Switches 001 and 002 FullTech
Maintenance and changes: <ul style="list-style-type: none">- What maintenance was performed before the incident and when- List of related changes applied before the incident and their details	Skyguide QBR 2022-02-22.pdf
	Skyguide QBR 2022-06-21.pdf
	Skyguide QBR 2022-09-20.pdf
Monthly service report for the last three months before the failure	Skyguide QBR 2022-02-22.pdf
	Skyguide QBR 2022-06-21.pdf
	Skyguide QBR 2022-09-20.pdf
List of current projects	List of NW projects
	Network Segregation Architecture v0.6.pdf
	1 Swiss airspace operations global OPS concept v1.0.pdf



BCM documents - specifically, the manual for testing the redundancies + how often is this carried out annually	2021-04-20 Assessment of Risk 35.4 Inability to provide core ATM services after a major disruption.pptx
	2022-06-15 EBCO Update BCM_COS.pptx
	3.1 Enterprise Risk Management - Corporate Top Risks – presentation.pdf
	CAP NASP Chapter 19 Audit with Scope on DXC Infrastructure
	Degraded_Modes_of_Operation.pdf
	M2WI0002E Business Impact Analysis.pdf
	M2WI0003E Business Continuity Plans.pdf
	M2WI0004E Crisis Organisation Skyguide.pdf
	M2WI0004E-A01_Job description Duty Officer COS.docm
	M2WI0004E-A02_Job description Chief of Staff COS.docm
	PO0100E Enterprise Risk Management Policy.pdf
	reference-guide-contingency-planning-ans-2009.pdf
	safety-guidelines-contingency-planning-ans-2009.pdf
	tA_Status_Report_ISMS_Initiatives_skyguide_645.pdf
Threat / Risk Matrix / prioritization related to BCM	DR0101E Enterprise Risk Management Directive.pdf
	EM - COS – BCM.pptx
	FOCA Questionnaire & SG Answers.pdf
	M2CL0002E_Employees to be mobilized for the Board of Crisis Management – BoC.pdf
	M2PD0001E Enterprise Risk Management.pdf
Information on training material on the process and how accessible the process is	Not available
Any regulatory requirements they need to fulfill in their Crises Management / INC Response if applicable	(Finding #55 - Draft Disaster Recovery Plan Building ANZ-A for phases 0 and 1).pdf



SDLC Process, Quality Gates within Release / Change Management processes until Transition Support with performance/failover Tests and Op. Readiness Tests	C2WI8011E_NELCH_(Innovation_&_Change_Management_-_Network_Services).pdf
	SOI Resilience assessment and Improvement V4.docx
Decision process and communication plan for Major Incident / Crisis Management / Disaster Recovery Process	M2MA0002M crisis com booklet.pdf
	M2CL0004E_Checklists for the Board of Crisis Management – BoC.docm
All communication in relation to the incident and crisis including	CAP NASP Chapter 19 Audit with Scope on DXC Infrastructure (Finding #55 - Draft Disaster Recovery Plan Building ANZ-A for phases 0 and 1).pdf
	2022 10 21 Crisis Communication Incident 15 June 2022 – Accenture.pptx
Investigation Report form S-Department	Incident 15 June All Internal Corporate Communications.pdf
	2022-06-15 Network Incident v1.0 released (without Mngmt responses.pdf
	2022-06-15 Network Incident v1.0 released (without Mngmt responses_Events_Highlighted.pdf
	2022-06-15 Network Incident v1.0 with T and O responses.pdf
	2022-06-22_Clear_the_sky_preliminary_report.pdf
Root Cause Analysis from Extreme Networks	2022-10-13 D Internal Safety Report 15 June 2022.final.pdf
	Skyguide RCA June15th2022 final.pdf
COS Lesson's Learned	2022-06-15 COS Event SYSTEM FAILURE CH - Review & Lessons Learned for COS V2022-07-09.pdf

Table 113: Information Basis



Software Release Versions



Platform	Installed	Maintenance Release	Latest Feature Release	Release Date
ERS 3500 Series	5.3.9.011	5.3.14.0	5.3.15.0	2021-11-02
ERS 4800 Series	5.12.2.011	5.12.6.007	5.12.6.007	2020-04-20
VSP4850 Series	VOSS 7.1.0.0	VOSS 7.1.10.0	VOSS 7.1.10.0	2021-06-11
VSP4450 Series	VOSS 7.1.0.0	VOSS 8.4.3.0	VOSS 8.5.0.0	2022-02-09
VSP7200 Series				
VSP7400 Series				
VSP8200 Series				
5420				
5520				
XMC	8.5.7.5 GTAC Release	8.5.7.28	8.5.7.28	2022-02-04
XIQ-SE	21.11.11.37	21.11.11.37	21.11.11.37	2022-02-02

©2021 EXTREME NETWORKS, INC. ALL RIGHTS RESERVED. 14

Figure 11: QBR Skyguide 22nd of February 2022 – Recommended Software

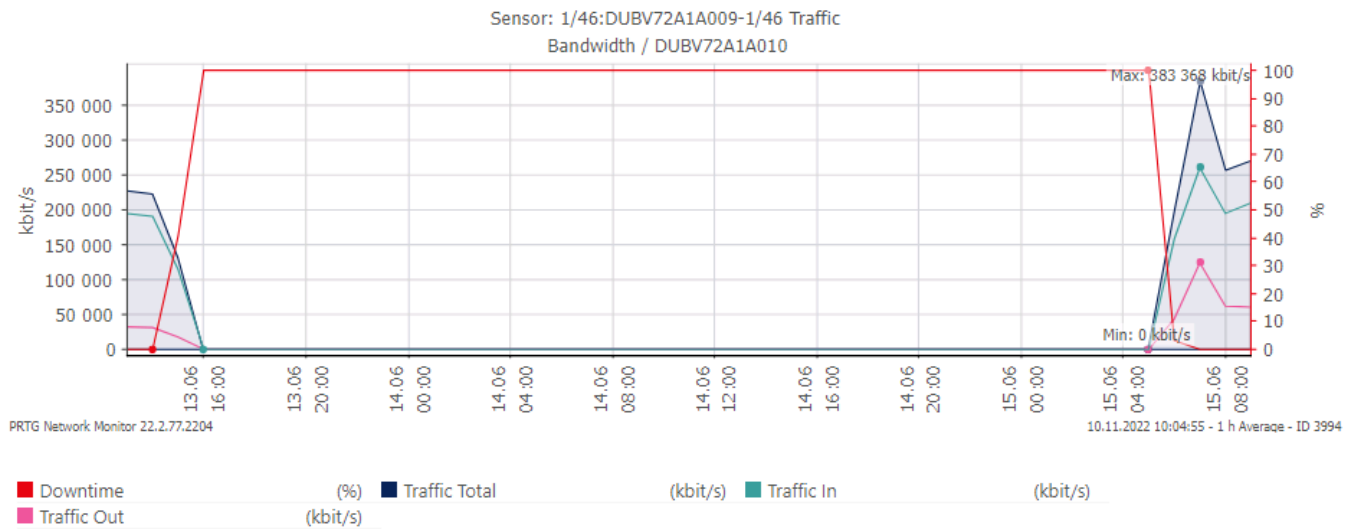


Figure 12: PRTG log for network switch 10 port 1/46 between 13th and 15th of June 2022

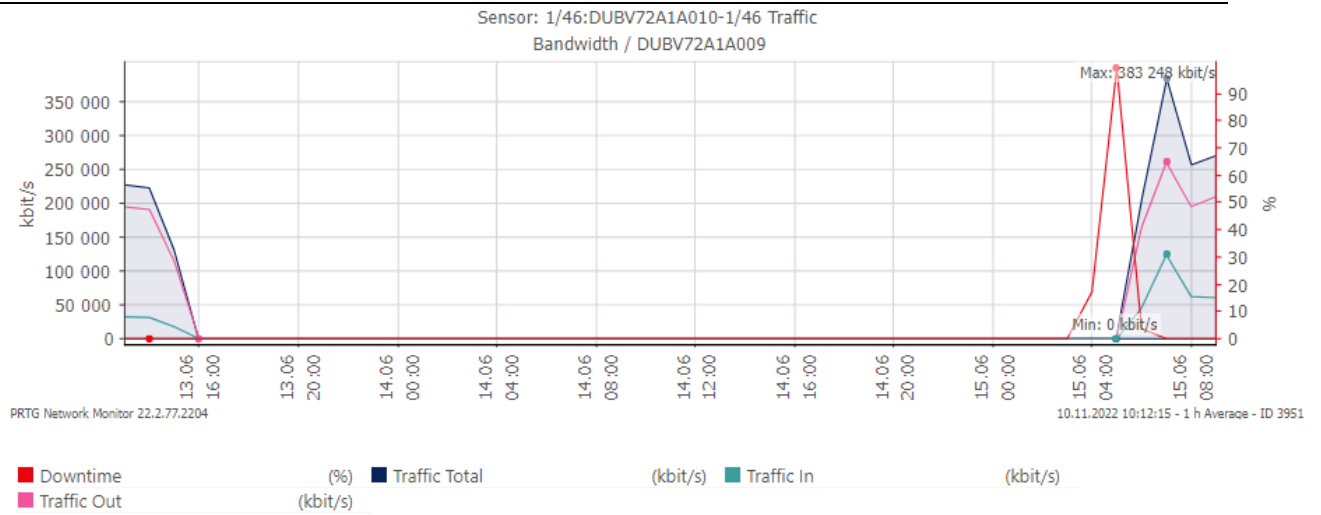


Figure 13: PRTG log for network switch 09 port 1/46 between 13th and 15th of June 2022

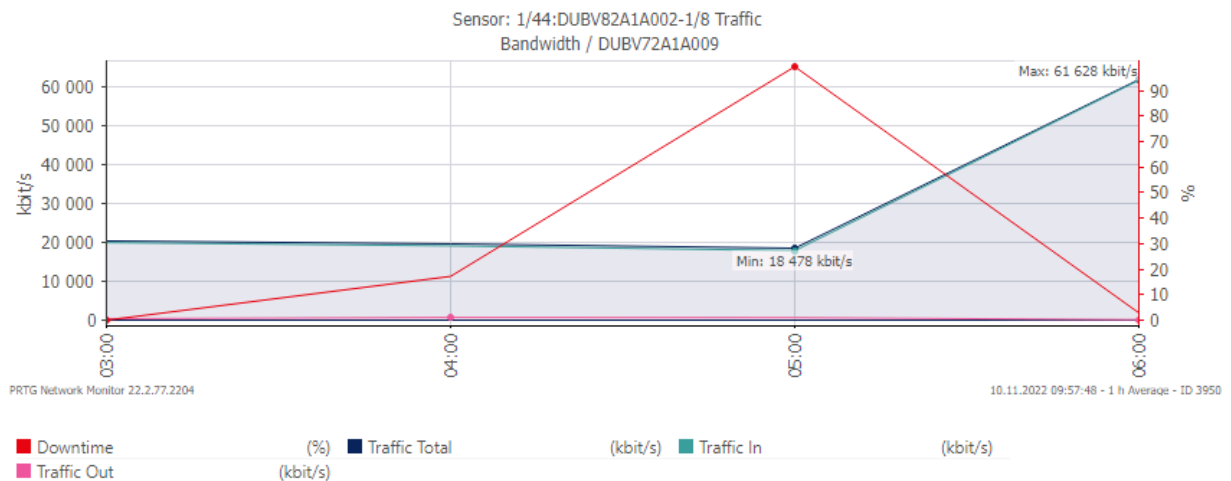


Figure 14: PRTG log for network switch 09 port 1/44 between 3:00am and 06:00am on 15th of June 2022



Component Details

Manufacturer: Avaya / Extreme
Type: Switch Layer 3
Device Name: * VSP 7254XSQ
Part number: * EC720001X-E6
Quantity of ports: 54
Description: Switch L3 54-port Ethernet Switch, supporting 48 x
Help on CI:

Current Authorization

Firmware	Software	ADMIN	OPS	TEST/LAB	VALID
VSP7200v8.5.1.0	All ERS/VSP License	Approved	Approved	Approved	Approved
VSP7200v7.1.0.0	All ERS/VSP License	End of Life	End of Life	End of Life	End of Life
VSP7200v6.0.1.2	All ERS/VSP License	Not approved	Not approved		Not approved
VSP7200v4.2.3	All ERS/VSP License	Not approved	Not approved		Not approved
VSP7200v4.2.1.1	All ERS/VSP License	Not approved	Not approved		Not approved
VSP7200v4.2.1.0	All ERS/VSP License	Not approved	Not approved		Not approved

Authorization History

Date	Firmware	Software	Domain	Authorization	Operator	Creation Date
23.09.2022	VSP7200v8.5.1.0	All ERS/VSP License	VALID	Approved	admin	22.11.2022
23.09.2022	VSP7200v8.5.1.0	All ERS/VSP License	TEST/LAB	Approved	admin	22.11.2022
23.09.2022	VSP7200v8.5.1.0	All ERS/VSP License	OPS	Approved	admin	22.11.2022
23.09.2022	VSP7200v8.5.1.0	All ERS/VSP License	ADMIN	Approved	admin	22.11.2022
23.09.2022	VSP7200v7.1.0.0	All ERS/VSP License	VALID	End of Life	admin	22.11.2022
23.09.2022	VSP7200v7.1.0.0	All ERS/VSP License	TEST/LAB	End of Life	admin	22.11.2022
23.09.2022	VSP7200v7.1.0.0	All ERS/VSP License	OPS	End of Life	admin	22.11.2022
23.09.2022	VSP7200v7.1.0.0	All ERS/VSP License	ADMIN	End of Life	admin	22.11.2022
06.03.2019	VSP7200v4.2.3	All ERS/VSP License	VALID	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.1	All ERS/VSP License	ADMIN	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.1	All ERS/VSP License	OPS	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.3	All ERS/VSP License	OPS	Not approved	admin	08.03.2019
06.03.2019	VSP7200v6.0.1.2	All ERS/VSP License	ADMIN	Not approved	admin	08.03.2019
06.03.2019	VSP7200v6.0.1.2	All ERS/VSP License	VALID	Not approved	admin	08.03.2019
06.03.2019	VSP7200v6.0.1.2	All ERS/VSP License	OPS	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.0	All ERS/VSP License	OPS	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.1	All ERS/VSP License	VALID	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.3	All ERS/VSP License	ADMIN	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.0	All ERS/VSP License	ADMIN	Not approved	admin	08.03.2019
06.03.2019	VSP7200v4.2.1.0	All ERS/VSP License	VALID	Not approved	admin	08.03.2019
15.11.2018	VSP7200v7.1.0.0	All ERS/VSP License	OPS	Approved	admin	15.11.2018
15.11.2018	VSP7200v7.1.0.0	All ERS/VSP License	ADMIN	Approved	admin	15.11.2018
24.10.2018	VSP7200v7.1.0.0	All ERS/VSP License	VALID	Approved	admin	24.10.2018
24.10.2018	VSP7200v7.1.0.0	All ERS/VSP License	OPS	Not approved	admin	24.10.2018
24.10.2018	VSP7200v7.1.0.0	All ERS/VSP License	ADMIN	In Test	admin	24.10.2018

Figure 15: Firmware level approval for 7200 model network switch



11. Appendix Timeline

Timeline of Events on 15 th of June 2022					
Time (UTC)	Action category	Action taken by	Action recipient	Verified	Action Comment
01:07	Incident Occurs	-	-	YES (Network Switch Logs)	Loss of connectivity.
01:07	Incident Occurs	Level 1 - SMC Geneva / Level 1 - SMC Zurich	-	YES (Ticket)	<p>Level 1 - SMC Geneva and Level 1 - SMC Zurich detecting many issues in their supervision monitor.</p> <p>Level 1 - SMC Zurich creating I220615_0001 with the following contents: "At 01:07utc System interruption on all important FDPZ, TRACE, Skyvisu, INCH ZRH & BRN (Bern), Farsight. iMON Supervision is lost."</p> <p>Level 1 - SMC Geneva creating I220615_0003 with the following contents: "At 01:07 major network failure. INIS, SYLEX, SYCO are down. iMON, and Smartradio supervision are lost."</p>
01:15	Escalation	Level 1 - SMC Zurich	Level 2 - Network	YES	Level 1 - SMC activates the on-call Level 2 - Network Operator in Zurich.



			Operations Zurich		
01:19	Escalation	Level 1 - SMC Geneva	Network Operations Geneva	YES	The Level 1 - SMC activates the on-call Level 2 – Network Operator in Geneva. He states that he has lost iMON and that Zurich has the same problem.
01:24	Internal Communication	SPVR Geneva	SPVR Zurich	YES	The supervisors align on the situation. They discuss about the Emergency manual and conclude that the maximal reduction suggested in the emergency manual is 40%. They agree that if they take a decision, they will take the same decision. They discuss that they should have until 04:00 UTC to inform Eurocontrol (NMOC).
01:31	Decision	SPVR ACC Zurich	INS-C / SPVR ACC Geneva	YES	The supervisor Zurich calls Geneva and informs that the systems in Zurich are not working for more than 5 minutes. Zurich does not have correlation and the SMC does not know what to do. Geneva does also have systems that are not working. They decide not to wait until 04:00 UTC and take the “Clear-the-Sky” action. SPVR Geneva proposes to call Eurocontrol (NMOC) and COS.
01:34	External Communication	SPVR ACC Geneva	Eurocontrol	YES	SPVR Geneva informs Eurocontrol (NMOC) about the system failure and sets rate ZERO for all traffic until 04:40 UTC.
01:37	Internal Communication	SPVR ACC Geneva	SPVR Zurich ACC	YES	SPVR Geneva informs SPVR Zurich that he has set the rate to ZERO and Zurich should do the same.



01:39	External Communication	SPVR ACC Zurich	Eurocontrol	YES	SPVR Zurich sets rate to ZERO for Zurich airspace (AZ airspace). He advises to set it similarly as for Geneva.
01:39	Escalation	COM Center	COS Duty Officer	YES (LogOps)	The COM Center was not able to reach the Duty Officer Geneva and instead they contacted the Duty Officer Zurich.
01:44	External Communication	SPVR ACC Zurich	ZRH Airport Steering	YES	SPRV Zurich starts to work through emergency checklist for "Clear-the-Sky" and informs Airport steering.
01:45	Internal Communication	Duty Officer Zurich	SPVR ACC Geneva	YES	Duty Officer Zurich checking the situation with Geneva to have baseline to decide.
01:57	Technical Resolution	Level 2 – Network Operations Geneva	Level 2 – Network Operations Zurich	YES (Interviews)	Handover of investigation lead from Level 2 – Network Operations Zurich to Level 2 – Network Operations Geneva.
02:00	Technical Resolution	Level 2 – Network Operations Zurich	BNC (Business Network Communications AG)	YES (Interviews)	Checking for firewall functionality with firewall vendor.



02:14	Internal Communication	Duty Office Geneva	COS	YES (Text message verified)	Info text message was sent.
02:17	Internal Communication	Duty Office Geneva	COS Zurich HQ	YES (Alerting Protocol)	COS Mobilization Zurich initiated
02:19	Internal Communication	Duty Office Geneva	COS Geneva HQ	YES (Alerting Protocol)	COS Mobilization Geneva initiated
02:40	External Communication	AIM (Aeronautical Information Management)	Austrocontrol	YES	First NOTAM published. COM Center Geneva sent an email to AIM. SCONE did not work because of the technical malfunction. Austria had to publish NOTAM.
02:35	Technical Resolution	Level 2 – Network Operations Geneva	-	YES (Interviews)	Level 2 – Network Operations Geneva started to investigate in the office in Geneva.



03:01	Decision	SPVR ACC Geneva	Eurocontrol	YES	The supervisor extends the zero rate until 06:00. In addition they agree to automatically extend the zero rate in steps of 30 minutes until further notice.
03:09	COS Orientation report	COS Zurich	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
03:24	Technical Resolution	Level 2 – Network Operatio ns and Level 3 – Network Engineeri ng	-	YES (Network Switch Logs)	Restart of switch DUBV82A1A002
03:39	Technical Resolution	Level 3 – Network Engineeri ng Team	-	YES (Interviews)	Level 3 - Network Engineering Team Geneva was engaged.
03:46	Technical Resolution	Level 2 – Network Operatio ns and Level 3 – Network	-	YES (Network Switch Logs)	Restart of switch DUBV82A1A001



		Engineering			
03:45	COS Meeting	COS	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
04:12	Technical Resolution	Level 2 – Network Operations and Level 3 – Network Engineering	-	YES (Network Switch Logs)	Turning off switch DUBV82A1A002
04:30	External Communication	Crisis Communication Group	Public Employees /	YES	Press release about the event published. Skyhub information about the event published for employees.
04:30	COS Meeting	-	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
04:51	Internal Communication	SPOC COS (Operations)	SPVR TWR/APP Geneva	YES	SPOC informs SPRV TWR/APP Geneva that they will be coordinator between COS and Operations



04:57	Technical Resolution	Level 2 – Network Operations and Level 3 – Network Engineering	-	YES (Network Switch Logs)	Switch DUBV82A1A002 starting again.
05:03	External Communication	Communication Department	Public	YES	Twitter post including the press release was published
05:03	Technical Resolution	Level 2 – Network Operations and Level 3 – Network Engineering	-	YES (Network Switch Logs)	Reboot of switch DUBV72A1A009. Network coming back up.
05:04	Internal Communications	Communication Department	All Employees	YES (Screenshot)	Internal E-Mail to employees on situation and reminder that no one should speak to media/public



05:05	Internal Communications	Communication Department	All Employees	YES (PDF Extract)	Intranet post on skyhub informing about the situation
05:05	Technical Resolution	Level 2 - Network Operations and Level 3 - Network Engineering	-	YES	Level 3 - Network Engineering Team started to investigate stability of the Network after improvements were identified.
05:09	Technical Resolution	Level 1 - SMC	-	YES (Protocol)	Level 1 - SMC detecting improvement in the monitoring console after DUBV72A1A009 has been rebooted.
05:15	COS Meeting	COS	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
05:30	Technical Resolution	Level 3 - Network Engineering Team	-	YES (Interviews)	Network was found to be stable. Monitoring ongoing.



05:50	COS Meeting	COS	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
06:08	Internal Communicati on	SPOC Operatio ns COS	SPVR TWR / APP Geneva	YES	SPOC informs that operations will start at 50% for the first hour and will then be increased to 75%
06:20	COS Meeting	COS	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
06:30	Clearance	COS	-	YES (Meeting Minutes)	Operations can be started again NOTAM can be cancelled.
06:29	Internal Communicati on	SPOC Operatio ns COS	SPVR TWR / APP Geneva	YES	SPOC COS communicated that operations can be started
06:34	External Communicati on	AIM	-	YES	NOTAM cancelled
07:30	COS Meeting	-	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5



07:53	Internal Communication	SPOC Operations COS	SPVR TWR/APP Geneva	YES	Capacity is allowed to run at 100% again
08:30	COS Meeting	-	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
10:00	COS Meeting	-	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5
12:00	COS Meeting	-	-	YES (Meeting Minutes)	Details on this meeting can be found in chapter 3.5

Table 114: Detailed Timeline



12. Appendix Key Definitions

Business Continuity – Strategic and tactical capability of the organization to plan for and respond to incidents in order to continue business operations at an acceptable pre-defined level.

Business Continuity Plan (BCP) – Documented collection of procedures and information that is developed, compiled and maintained in readiness for use during a large-scale enterprise or functional business-impacting event and enabling an organization to continue delivery of its critical activities at an acceptable, pre-defined level. Similarly is also defined ICT (business) Continuity Plan.

Business Continuity Plan Management Team (BCP MT) - The tactical team that would respond in an incident, and that should contribute significantly to the writing and testing of Business Continuity Plan. Similarly, is also defined ICT (business) Continuity Plan Team.

Disaster – specific to ICT continuity, it is a by authorized person declared situation which requires invocation of ICT DR Plan.

Disaster Recovery Plan Management Team (DRP MT) – The tactical team that would respond in an IT technical incident, and that should contribute significantly to the writing and testing of Disaster Recovery Plan.

Disaster Recovery (DR) - Activities and programs that are invoked in response to a disruption and are intended to restore an organization's ICT services (technical part of ICT Continuity).

ICT Continuity – Capability of the organization to plan for and respond to incidents and disruptions on order to continue ICT services at an acceptable preferred level. ICT Continuity is business continuity for ICT service provider.

ICT (business) Continuity Plan (ICT CP) – see BCP

Incident - Situation that might be, or could lead to, a business disruption, loss, emergency, crisis or disaster.

Recovery Time Objective (RTO) - The target timeframe within which delivery of a product or service must be recovered following some form of catastrophic disruption to delivery sustainable capability. $RTO \leq MTPoD$.



Recovery Point Objective (RPO) – The target timeframe established for the recovery and availability of data (electronic data and hardcopy) as part of the overall recovery process.
RPO ≤ MTDL

Recovery Time Capability (RTC) – it is real recovery duration which is result of a test.

Business Recovery Plan (BRP) - Document that provides vital information and detailed procedures for each Business Recovery Team to support recovery and continuity of critical business functions in the event of a disruption.

Business Recovery Team (BRT) - Various business operations teams necessary to recover a business function disrupted at the primary location at the secondary location. Each BRT is comprised of operations staff and subject matter experts from their operations group.



13. Appendix Questions

This chapter shows the questions listed in the book of specification.

13.1. Technische Störung

Unabhängige Untersuchung der technischen Störung (Problem mit dem «Core Switch Cluster» in Dübendorf). Im Rahmen der Untersuchung sind insbesondere die folgenden Fragen

zu beantworten:

1. Was genau war das technische Problem und was war die Ursache?
2. War das Ereignis vorhersehbar?
3. Hat skyguide die richtigen technischen Abhilfemassnahmen zur richtigen Zeit und schnell genug eingeleitet?
4. Waren die Prozesse, mit denen die Abhilfemassnahmen eingeleitet wurden, vorhanden, angemessen und wirksam?
5. Waren Wartungsverfahren vorhanden, wurden sie angewendet und waren sie wirksam? Hätten die jetzt vorgenommenen Updates früher durchgeführt werden sollen?
6. Erlaubte es die technische Infrastruktur, die richtigen Abhilfemassnahmen zu identifizieren?
7. Wurde das Funktionsverhalten im eingeschränkten Betrieb («degraded modes») vorhergesagt und spezifiziert?
8. Gab es genügend Redundanz in der technischen Infrastruktur, die eine Fehlfunktion aufwies?
9. Waren die Methoden zur Analyse der Architektur angemessen?
10. Wurden bei der Analyse einzelne Fehlerpunkte der Architektur identifiziert?
11. Wurde die Redundanz analysiert und war sie für die Entkopplung («Isolation») der Systeme angemessen?
12. Wie kann eine solche Situation in Zukunft verhindert werden?
13. Wie können ähnliche Situationen frühzeitig identifiziert werden?
14. Die Ergebnisse der internen Untersuchung von skyguide sind ebenfalls in Frage zu stellen: Bestätigen die gesammelten Informationen die Ergebnisse der internen Untersuchung von skyguide (technische Berichte / Sicherheitsuntersuchungsbericht) oder nicht?



13.2. Krisenmanagement

Untersuchung des Krisenmanagements, insbesondere bezüglich der folgenden Fragestellungen:

- 15. Wurde der COS-Prozess (Crisis Organisation skyguide) eingehalten?
- 16. Wie war die Zusammenarbeit, die Kommunikation und der Entscheidungsprozess innerhalb des COS-Teams?
- 17. Wurden die Stakeholder (intern/extern) nach ihrer eigenen Meinung ausreichend informiert?



14. Appendix Abbreviations

Abbreviation	Definition
ACC	Area Control Center
AIM	Aeronautical Information Management
AIRAC	Aeronautical Information Regulation and Control
ANS	Air Navigation Service
ASIC	Application Specific Integrated Circuit
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
BCM	Business Continuity Management
BIA	Business Impact Assessment
BNC	Business Network Communications AG
BoC	Board of Crisis
BRN	Bern
CEO	Chief Executive Officer
CIR	Common IFR Room
CMDB	Configuration Management Database
CNS	Communication, Navigation, Surveillance
COM	Communication
COO	Chief Operating Officer
COS	Crisis Organization skyguide
DDPS	Federal Department of Defense, Civil Protection and Sport
DETEC	Federal Department of the Environment, Transport, Energy and Communications
DO	Duty Officer
DR	Disaster Recovery
DUB	Dübendorf
ECMT	Electronic Crisis Management Tool
EM	Emergency Management
EoL	End of Life
EoS	End of Support
ESX/ESXi	Physical servers hosting virtual machines
EVACO	Evacuation
FDPZ	Flight Data Processing application in Zürich
FIC	Flight Information Center
FLAS	Flight Allocation Scheme
FOCA	Federal Office of Civil Aviation
FZAG	Zürich Airport
GS	General Secretary
GVA	Geneva
HA	High Availability
HQ	Head Quarter
IFR	Instrument Flight Rules
iMON	Integrated MONitoring (Monitoring tool)
INC	Incident (response)
INCH	Information CH – application for environmental data



INIS	Interface IFPS-SYCO
IS-IS	Intermediate System to Intermediate System
iSUP	Integrated Supervision – Main supervision for SMC
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MPLS	Multiprotocol Label Switching
MTPoD	Maximum Tolerable Period of Disruption
NMOC	Network Manager Operations Center
NOTAM	Notice to Airmen
NTSB	National Transportation Safety Board
OLG	Head of Tower/Approach Geneva
OPS	Operations
PIN	Personal Information Number
PRTG	Network monitoring application
QBR	Quarterly Business Review
RADIUS	Remote Authentication Dial-In User Service
SCONE	Skyguide equipment used to publish NOTAMs
SDLC	Software Development Life Cycle
SLA	Service-Level Agreement
SMC	Systems Monitoring and Control
SME	Subject Matter Expert
SMS	Short Message Service
SPOC	Single Point of Contact
SPVR	Supervisor
STSB	Swiss Transportation Safety Investigation Board
SYCO	Système de Coordination
SYLEX	Système de Liaison Externe
TRACE	ZRH TWR/APP FDP application
TWR	Tower
UPS	Uninterruptible Power Supply
VFR	Visual Flight Rule
vIST	Virtual Inter-Switch Trunk
Vlcp	Virtual Link Aggregation Control Protocol
WAN	Wide Area Network
WTO	World Trade Organization
XIQ	Extreme Networks monitoring - ExtremeCloud IQ
ZRH	Zürich

Table 115: Abbreviations



15. Appendix Overview Interviews

The following table provides an overview of interviews conducted during this investigation:

Part	Topic	Skyguide Roles	Date	Time
BCM and DR	IT Infrastructure to Business Process Mapping	Head of Enterprise Architecture	20.10.2022	11:30 – 11:55
BCM and DR	Internal and External Communication	Communication	24.10.2022	13:00 – 14:00
		Communication		
		Communication		
Network	Architecture and Design Principles	Network Architect	25.10.2022	08:30 – 09:30
Network	Investigation of incident occurred on the 13 and 15.06	Network Engineer	25.10.2022	10:00 – 12:00
		Network Engineer		
		Network Engineer		
Network	Service Delivery and Monitoring	Service Delivery	25.10.2022	13:00 – 14:00
		Lead Monitoring		
Network	Network Operation and Monitoring	Team Lead Operation	25.10.2022	14:15 – 15:15
BCM and DR	Crisis Management, BCM and Disaster Recovery	PoC to OPS Zurich	26.10.2022	08:30 – 09:30
		Chief of Staff		
		BCM Lead		
BCM and DR	System Resiliency and Architecture	Lead System Resiliency	26.10.2022	13:00 – 14:00
		Lead Overall Investigation		
BCM and DR	Air Traffic Control and Operation	Lead Air Traffic Control	26.10.2022	14:30 – 15:30
Network	Overall network root cause analysis	Network Architect	27.10.2022	13:00 – 14:30
		Overall Investigation Lead		
BCM and DR	Timeline and Event Series	BCM Lead	28.10.2022	08:00 – 09:00
BCM and DR	Timeline and Event Series	BCM Lead	03.11.2022	08:30 – 09:30
BCM and DR	Supervisor Zurich 1/2	Supervisor ZRH 1	07.11.2022	09:30 – 10:00
Com	Airport Zurich (FZAG)	-	07.11.2022	16:30 – 16:50
Network	Network Operation and Monitoring	Team Lead Operation	08.11.2022	13:00 – 14:00
SPV ZH 2	Supervisor Zurich 2/2	SPV ZRH 2	09.11.2022	08:30 – 09:00
Network	Network Operation Monitoring Capabilities	Network Operation SME	09.11.2022	08:30 – 10:30



Com	FOCA	-	10.11.2022	08:30 – 09:00
BCM and DR	Supervisor Geneva	Supervisor Geneva	10.11.2022	09:00 – 10:00
Network	Network Operation Monitoring Capabilities	Network Operation SME	10.11.2022	10:30 – 13:00
BCM and DR	NOTAM Publication and Duty officer notification	Head AIM	10.11.2022	14:00 – 15:00
BCM and DR	Supervisor Geneva	Supervisor Geneva	10.11.2022	15:00 – 15:35
Com	DETEC	-	11.11.2022	10:00 – 10:15
Com	Communication	Chairman of the Board	11.11.2022	14:30 – 14:50
BCM and DR	Supervisor Geneva	Supervisor Geneva	16.11.2022	10:00 – 10:45
Com	Airport Geneva	-	17.11.2022	08:30 – 08:50
Com	Swiss Airlines	-	23.11.2022	08:30 – 09:00

Table 116: Overview of Interviews

