1. Introduction

This document lays down the basic principles for defining and measuring service quality, controlling service provision and confirming the performance of the ICT services of Swisscom (Switzerland) Ltd, hereinafter referred to as «Swisscom».

Based on this, the following points can be defined for each service in the relevant individual contracts:

- The Service Level Metrics and Target Values that represent qualitative requirements for the service quality;
- The measurement procedures used to verify compliance with the Service Levels;
- The Standard Service Level report, which contains periodic evaluations of the agreed Service Levels as proof of the services provided by Swisscom.

2. General definitions

2.1. Standard Service Level Parameters (SSLP)

SSLPs provides a thematic grouping of Service Levels.

2.2. Service Level

The Service Level is used to define the service quality and the measurement, control and proof thereof. The Service Level is defined by a Service Level Metric and a Service Level Target Value.

2.3. Service Level Metric

The Service Level Metric defines how the service quality of the provided service is calculated quantitatively.

2.4. Service Level Target Value

The Service Level Target Value is the value to be attained by Swisscom for the relevant Service Level.

2.5. Service Access Interface Point (SAIP)

The SAIP is the geographic and/or logical point at or up to which a service is provided to the Customer, monitored and accounted for.

2.6. Service Level Agreement (SLA)

An SLA is an agreement reached between Swisscom and the Customer in an individual contract regarding the SAIPs, SSLPs, Service Levels and their Target Values applicable to service provision.

The following diagram illustrates an SLA that includes Service Level Metrics and Service Level Target Values for each service:

Service Level Agreement (SLA)

Service	Quality attributes	Quality targets
Specifications	Service Level Metric	Service Level Target
Service A	Service Availability	99.9%
	Service Outages	1
Service B	Incident Intervention Time	Best Effort

2.7. Best Effort

If no Service Level Target Value is specified, the Target Value is Best Effort.

The only exception to this is the Service Level RPO (Recovery Point Objective) for the SSLP continuity, in which no specification of a Target Value means that the RPO is not supported (i.e. Not Available).

Service Levels with the Target Value «Best Effort» are not measured and therefore not listed in a Service Level report. Any exceptions are set out in the respective individual contract.

2.8. Reporting period

The reporting period is the period in which the service quality is measured and compliance with the Service Level Target Values is verified. Proof of quality is provided by means of a standard Service Level Report.

Unless defined otherwise in the individual contract, the reporting period is set at one calendar month.

2.9. Business Day (EONBD, EOxBD)

The Business Day is defined by the agreed Support Time (weekday or start and end of the Business Day).

End of Next Business Day, end of X business days: The end of a promised period, whereby «X» defines the duration (i.e. the number of days).

2.10. Holiday regulations

The following are public holidays: 1 January, Ascension Day, 1 August and 25 December. The cantonal public holidays at the place of performance also apply. Individual deviations, especially at international locations, are defined in the relevant individual contract.

2.11. Incidents and Incident Management Process

Incidents are events that are not part of standard operations and either restrict or potentially restrict the service quality or the Customer's productivity. There are two different types of fault report with regard to incidents:

- User-Driven: A user or the Customer reports a fault via the channels defined in the contract or specified by Swisscom;
- System-Driven: A system reports a fault and automatically generates an incident ticket on the ticket system.

Within the Incident Management Process, the duration of a fault between the Time Stamp «Ticket Created Start Incident T0» and «Incident Resolved Time Stamp » is recorded in an incident ticket. This information is used to, among other things, calculate the Availability and for Service Level Reporting.

Workarounds are considered temporary fault rectification. If the Customer can use the service it is considered to be available during that time.

2.12. Suspend Time

Suspend Time is the period of time in [hh:mm] during which fault rectification or request fulfilment is paused. It is not included in the Service Level calculation. Reasons for this include:

- Service Outages and Service Requests outside the agreed Support Times.
- The outage falls within a Provider Maintenance Window used by Swisscom or a customer specific maintenance window or within an announced service interruption.
- The fault is due to an external system error or interruption of internet access, the rectification of which does not fall within Swisscom's performance obligation.
- Swisscom can show that neither it nor its auxiliaries are to blame for the outage.
- In the event of a False Alarm. The incident ticket is closed on the grounds «False Alarm».
- Periods of reduced performance (latency/transmission delays, throughput packet loss, etc.), if measurements made by Swisscom show that the contractually specified values were reached.
- The Customer or third parties commissioned by the Customer has/have rights that could potentially adversely affect compliance with the SLA (namely root/admin rights on the systems operated by Swisscom).
- The Customer is not available to support or complete fault rectification within the context of its duty to cooperate. For example, if the Incident Management Process cannot be complied with because the Customer cannot be contacted, or if it is inaccessible or fails to provide confirmation. This applies in particular if the Customer has not updated the information on its contacts.
- The Customer's provision obligations have not been met.
- During fault rectification, the Customer is identified as being responsible for the fault. For example:
  - Applications, equipment or facilities which are not part of the agreed scope of the services (this also applies to equipment provided by the Customer, e.g. in the event of faults in the software licenced by the Customer) or services provided by third parties commissioned by the Customer.
  - On-site faults: For example, involving in-house installations, the Customer's network, electricity and/or cooling systems, improper handling by the Customer, etc.
- Postponement of the appointment by the Customer.

2.13. Ticket

A ticket contains detailed information about a fault, Problem, Change or Service Request. Incident tickets provide information on the life cycle of a single fault, for example.

2.14. Time zones

Unless expressly stated or agreed, time indications refer to the Swiss time zone.

3. Standard Service Level Parameters (SSLP)

3.1. SSLP Operation Time

3.1.1. Definition

The «SSLP Operation Time» parameter is the period in which all technical service components relevant for the service provision are in operation. This is usually Mo–Su 00:00-24:00 excl. maintenance windows. Compliance with the operating time is not reported.

SSLP Operation Time	In the individual contract	Definition
Example values[1]	Mo-Su 00:00-24:00	Monday-Sunday, 24 hours a day, incl. public holidays but excl. maintenance windows

3.1.2. Maintenance Windows

Maintenance Windows are used to reserve periods for maintenance activities by Swisscom. These periods are only used when there is a specific need. Swisscom makes every effort to keep service interruptions which are genuinely necessary as short as possible.

Swisscom distinguishes between

- Provider Maintenance Windows (PMWs) at Swisscom Data Centers
- Provider Maintenance Windows for networks between customer sites and Swisscom
- Service-specific maintenance windows and
- Customer-specific maintenance windows

Comments:

- The Customer must ensure that no customer-side maintenance work is planned or carried out during these times.
- In general, incident tickets are not used during maintenance windows.
- Once maintenance work has been completed, Swisscom tests/verifies the functionality of the services for which it is responsible. All other services – i.e. those that are not Swisscom's responsibility – must be tested by the Customer.

3.1.2.1. Provider Maintenance Windows at Swisscom Data Centers

Provider Maintenance Windows at Swisscom Data Centers (PMW-DC) are used to reserve periods for maintenance activities at Swisscom's Data Centers.

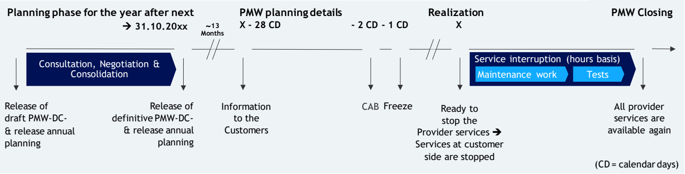
The following three types of Provider Maintenance Windows are possible at Data Centers:

PMWs at Swisscom Data Centers (PMW-DC)			
Type	Description	Reserved timeframe	Service interruptions
General (GPMW)	For maintenance work on the DC infrastructure[2]	Per year, 8 weekends each Sa 18:00 – Su 18:00	Usually no service interruptions or only short ones
Connectivity (CPMW)	For maintenance work on the network within Swisscom Data Centers	4 weekends a year at 3 nights each: Fr 22:00 – Sa 06:00 and Sa 22:00 – Su 07:00 and Su 22:00 – Mo 06:00	Usually <1 hour
Backup	For maintenance work on the backup infrastructure	Weekly We 14:00-17:00	Usually no service interruptions or only short interruptions

These maintenance windows apply to all services produced within Swisscom Data Centers. Service-specific maintenance windows also apply.

The process for planning a PMW-DC (general and connectivity) is as follows:

Swisscom informs the Customer about the PMW-DC (general and connectivity) in the planning phase. The dates are set by 31 October of the year before last (14 months in advance) in the annual PMW-DC and release plans:


Planning phase for the year after next
→ 31.10.20xx
~13 Months
PMW planning details
X - 28 CD
- 2 CD - 1 CD
Realization
X
PMW Closing
Consultation, Negotiation & Consolidation
Service interruption (hours basis)
Maintenance work
Tests
Release of draft PMW-DC- & release annual planning
Release of definitive PMW-DC- & release annual planning
Information to the Customers
CAB
Freeze
Ready to stop the Provider services → Services at customer side are stopped
All provider services are available again
(CD = calendar days)

Detailed planning is conducted prior to each maintenance window. As part of this, the forthcoming maintenance work, the specific service interruptions and the planned duration are defined and communicated to the Customer 28 calendar days in advance. The system change is given final approval at the next meeting of the Change Advisory Board (CAB).

No coordination with the Customer is envisaged for PMW-DC backup maintenance windows because they have no impact on service performance.

3.1.2.2. Provider Maintenance Windows for networks between the Customer's sites and Swisscom

The Provider Maintenance Window for the networks between the Customer's sites and Swisscom (PMW-NWK) is the time period which is generally used by Swisscom for conducting maintenance work on the network platform outside the Data Centers.

PMWs for networks between the Customer's sites and Swisscom (PMW-NWK)		
Connectivity	For maintenance work conducted on Swisscom networks outside the Data Centers	Weekly Su 02:00-06:00

Connectivity may possibly, but not necessarily, be affected during such maintenance. The Customer is given advance notice of any scheduled interruptions within the maintenance window which are expected to last longer than specified in the individual contract. In all other cases, the Customer is not notified specially about maintenance work.

3.1.2.3. Service-specific Provider Maintenance Windows

The Provider Maintenance Windows of the individual services (PMW-S) are used to maintain the service-specific infrastructure. They are set out in the individual contract.

Service-specific Maintenance Windows (PMW-S)		
Service platform	For maintenance work conducted on the Swisscom platforms used to provide the service.	Specified in the individual contract.

Unless stipulated otherwise in the individual contract, no coordination with the Customer takes place.

3.1.2.4. Customer-specific maintenance windows

Customer-specific maintenance windows (IMW) for customer-specific ICT infrastructure and applications are coordinated and agreed mutually.

Customer-specific Maintenance Windows (IMW)		
Individual	For maintenance work on customer-specific ICT infrastructure and applications at customer sites.	By agreement

If not included in a corresponding Swisscom service, the corresponding maintenance work is specified, agreed and invoiced on a project basis, taking the associated additional work into account.

3.1.3. Emergency System Changes

Short-term Emergency System Changes may be required for all ICT components during operation, but outside the PMW. Swisscom therefore reserves the right to carry out unscheduled Emergency System Changes such as security patches immediately.

Where possible, customers are informed shortly before the implementation of emergency system changes. If an emergency system change affects a system dedicated to the Customer, the Customer has the right of veto[3] and can demand an alternative date for the installation. In this case, the Customer bears all associated risks itself. After an Emergency System Change has been carried out, a final message is sent to the Customer.

[1] The specific target values are defined for each service in the individual contract.

[2] Building, heating, ventilation, air conditioning, power supply, etc.

[3] Veto rights cannot be offered for systems that are shared by multiple customers.

3.2. SSLP Support Time

3.2.1. Definition

The «SSLP Support Time» parameter defines the time period (from-to) during which

- Qualified staff are available for interventions and any necessary fault rectification, i.e. the contractually agreed Service Levels are guaranteed during this time;
- Compliance with the Service Level Agreement is evaluated and verified as part of Service Level Reporting;

or

- Further agreed process-related and personal services are provided (e.g. in case of use within the framework of professional services, consultancy, etc.)

The period outside the Support Time is always considered Suspend Time.

For the «SSLP Support Time» parameter, different profiles are available depending on the service.

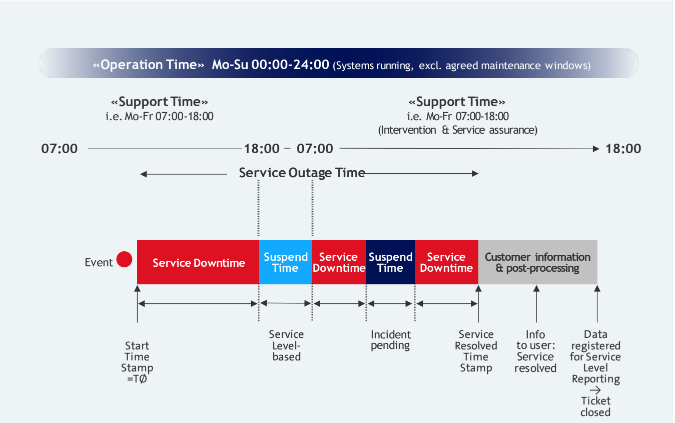
SSLP Support Time	In the individual contract	Definition
Example values[1]	Mo-Fr 07:00-18:00	Monday to Friday from 7 a.m. to 6 p.m.
	Mo-Sa 06:00-22:00	Monday to Saturday from 6 a.m. to 10 p.m.
	Mo-Su 00:00-24:00	Monday to Sunday, 24 hours a day

Holidays are generally excluded from the Support Time, except in the case of Mo-Su 00:00-24:00 which includes public holidays. Any deviations from this rule are set out in the individual contract.

3.3. SSLP Availability

3.3.1. Definition

The «SSLP Availability» parameter denotes the availability of the service at the defined SAIP. The following diagram shows the relation of the different times for SSLP Availability:


«Operation Time» Mo-Su 00:00-24:00 (Systems running, excl. agreed maintenance windows)
«Support Time» i.e. Mo-Fr 07:00-18:00
«Support Time» i.e. Mo-Fr 07:00-18:00 (Intervention & Service assurance)
07:00
18:00 – 07:00
18:00
Service Outage Time
Event
Service Downtime
Suspend Time
Service Downtime
Suspend Time
Service Downtime
Customer information & post-processing
Start Time Stamp =TØ
Service Level-based
Incident pending
Service Resolved Time Stamp
Info to user: Service resolved
Data registered for Service Level Reporting → Ticket closed

The «Service Outage Time» is the total period during which the service is unavailable. It includes the gross time of a Service Downtime, i.e. independent of the agreed support and Suspend Time.

Service Downtime [h:m]

The «Service Downtime » Service Level is usually used for business-related services. It determines the sum of the individual Service Downtimes during the Support Time, minus the Suspend Time, within a reporting period.

SSLP Availability	Service Downtime [h:m]
Metric	Service Downtime in h:m = ∑ Service Outage Time - ∑ Suspend Time
Example values[1]	1 h

Service Availability [%]

The «Service Availability» Service Level is usually used for infrastructure-oriented services. It shows the Service Availability during a reporting period as a percentage.

SSLP Availability	Service Availability [%]
Metric	Service Availability in % = $\frac{\text{Operation Times - (∑ Service Outage Times - ∑ Suspend Times)}}{\text{Operation Times}} \times 100$ [4]
Example values[1]	99.99%

Service Outage [#]

The «Service Outage» Service Level measures the number of Service Level-relevant outages per reporting period:

SSLP Availability	Service Outage [#]
Metric	Service Outage = The number of Service Level relevant outages
Example values[1]	1

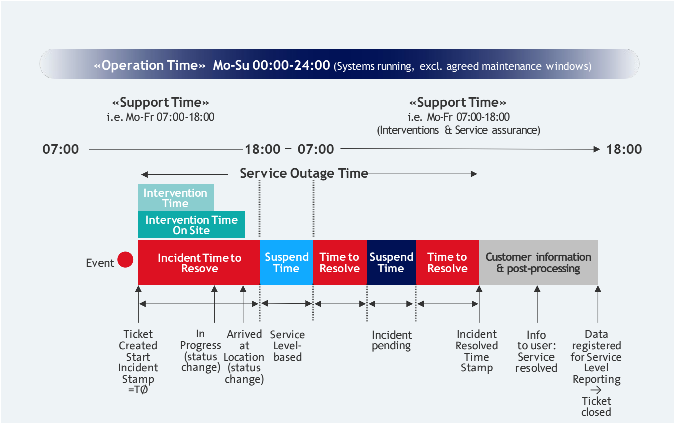
Multiple Service Outages with the same root cause within a given reporting period are considered as one Service Outage.

3.4. SSLP Process

The «SSLP Process» parameter defines Service Levels to measure, control and report process performance (e.g. ITIL or business processes).

3.4.1. Incident Management Process

The following diagram shows the relationship between the different times for the Incident Management Process:


«Operation Time» Mo-Su 00:00-24:00 (Systems running, excl. agreed maintenance windows)
«Support Time» i.e. Mo-Fr 07:00-18:00
«Support Time» i.e. Mo-Fr 07:00-18:00 (Interventions & Service assurance)
07:00
18:00 – 07:00
18:00
Service Outage Time
Intervention Time
Intervention Time On Site
Event
Incident Time to Resove
Suspend Time
Time to Resolve
Suspend Time
Time to Resolve
Customer information & post-processing
Ticket Created Start Incident Stamp =TØ
In Progress (status change)
Arrived at Location (status change)
Service Level-based
Incident pending
Incident Resolved Time Stamp
Info to user: Service resolved
Data registered for Service Level Reporting → Ticket closed

The calculation of the Service Levels «Incident Intervention Time», «Incident Intervention Time On Site» and «Incident Time To Resolve» for each fault is based on the evaluation of the incident tickets over the reporting period.

When an incident ticket is entered, the incident's priority is determined in accordance with established procedures. This can be done together with the Customer and/or based on information provided by the Customer when reporting the fault.

The incident's priority (3) is determined in terms of its Impact (1) and Urgency (2) as defined in the following tables:

(1) Impact:

Impact Level	Definition
1 - Severe	All users are affected and unable to do their work and/or severely hampered in some way.
2 - Significant	A large proportion of users is affected.
3 - Moderate	One or more users are affected.
4 - Minor	No users are affected yet.

[4] For the Operation Time, the number of days per month (28, 29, 30, 31) is differentiated in the calculation.

(2) Urgency:

Urgency Level	Definition
1 - Very Urgent	The criticality of the incident is «very urgent»: • The (financial) impact of the incident is increasing very quickly. • Work that cannot be completed due to the incident is extremely time critical.
2 - Urgent	The criticality of the incident is «urgent»: • The (financial) impact of the incident is increasing quickly. • Work that cannot be completed due to the incident is time critical.
3 - Standard	The criticality of the incident is «normal»: • The (financial) impact of the incident is increasing significantly over time. • Work that cannot be completed due to the incident is somewhat time critical.
4 - Not Urgent	The incident is not time-sensitive: • The (financial) impact of the incident is increasing only slightly over time. • Work that cannot be completed due to the incident is not time critical.

(3) The Impact and Urgency together generate the incident priority matrix:

Impact	1 – Severe	3 – Medium	2 – High	1 – Critical	1 – Critical
	2 – Significant	3 – Medium	3 – Medium	2 – High	1 – Critical
	3 – Moderate	4 – Low	3 – Medium	2 – High	2 – High
	4 – Minor	4 – Low	4 – Low	3 – Medium	2 – High
Priority		4 – Not Urgent	3 – Standard	2 – Urgent	1 – Very Urgent
		Urgency			

Incident Intervention Time [h:m, BD]

The «Incident Intervention Time» Service Level defines the length of time per fault between the «Ticket Created» and «In Progress» time stamps, minus the Suspend Time:

SSLP Incident Management Process	Incident Intervention Time [h:m, BD]
Metric	Incident Intervention Time per incident [h:m, BD] = «In Progress» time stamp - «Ticket Created» time stamp - ∑ Suspend Time(s)
Example values[1]	Critical: 15 min; High: 1 h; Medium: 4 h; Low: EONBD

Incident Intervention Time On Site [h:m, BD]

The «Incident Intervention Time On Site» Service Level defines the duration per incident between the «Ticket Created» and «Arrived at Location» time stamps, minus Suspend Time:

SSLP Incident Management Process	Incident Intervention Time On Site [h:m, BD]
Metric	Incident Intervention Time On Site per incident [h:m, BD] = «Arrived at Location» time stamp - «Ticket Created» time stamp - ∑ Suspend Time(s)
Example values[1]	Critical: 2 h; High: 4 h; Medium: 8 h; Low: EO2BD

Incident Time to Resolve [h:m, BD]

The «Incident Time to Resolve» Service Level defines the duration from opening the ticket to fault rectification, minus Suspend Time, for each fault:

SSLP Incident Management Process	Incident Time to Resolve [h:m, BD]
Metric	Incident Time to Resolve [h:m, BD] per incident = Service Downtime - ∑ Suspend Time(s)
Example values[1]	Critical: 4 h; High: 8 h; Medium: EONBD; Low: EO2BD

3.4.2. Service Request Process

A Service Request is a demand by an authorised employee of the Customer for information or a service specified in the customer Service Request catalogue.

A Service Request always refers to a contractually agreed service which has at least been partially transferred into operation.

Service Requests are carried out Mo-Fr 08:00-17:00. Exceptions are listed in the individual contract.

The IMACD Service Request defined below is a typical use case.

IMACD Fulfillment Time [h:m, BD]

IMACD (Install, Move, Add, Change, Dispose) are standardised service packages/changes that are offered for commissioning, changing, reducing, extending or dismantling a service.

The «IMACD Fulfillment Time» Service Level defines the period from the placement of the order on the system to the completion of an IMACD Service Request:

SSLP Process - Service Request Process	IMACD Fulfillment Time [h:m, BD]
Metric	IMACD Fulfillment Time [h:m, BD] = «Request Completed» time stamp - «Request Created» time stamp - ∑ Suspend Time(s)
Example values[1]	8 h, EO2BD

3.4.3. Service Fulfillment Process

Ready for Service (RFS) [Date]

The «Ready for Service» Service Level defines the date, confirmed by Swisscom, on which the contractually agreed service will be ready for use. The precise date can be agreed contractually.

The «Ready For Service» Service Level defines the agreed provision date:

SSLP Service Fulfilment Process	Ready For Service (RFS) [date]
Example values[1]	1.2.2020, 14 days after order

3.5. SSLP Performance

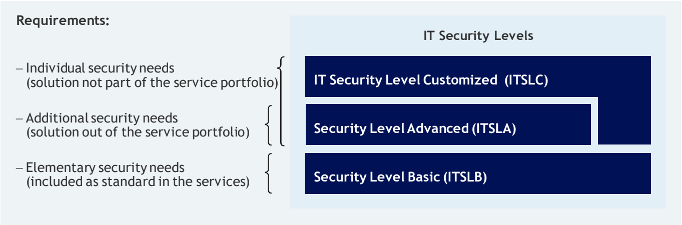
The «SSLP Performance» parameter provides information about the degree of utilisation, the throughput, measurements and response times of reference transactions and their quantities (activities and transactions). For such performance measurements, supplementary technologies such as probes, agents, recorders and/or robots as well as monitoring systems are used as required at the Swisscom data centre and/or on the customer side.

The agreements regarding the measurement criteria and procedure, preparation of the Service Level report and the conditions can be defined individually in the individual contract.

3.6. SSLP Security

The «SSLP Security» parameter covers several levels of protection that take the various ICT security requirements into account. The defined protection levels describe security measures used to implement the following protection objectives: confidentiality, integrity, obligation and availability.

The following illustration compares the protection requirements with the IT security levels:

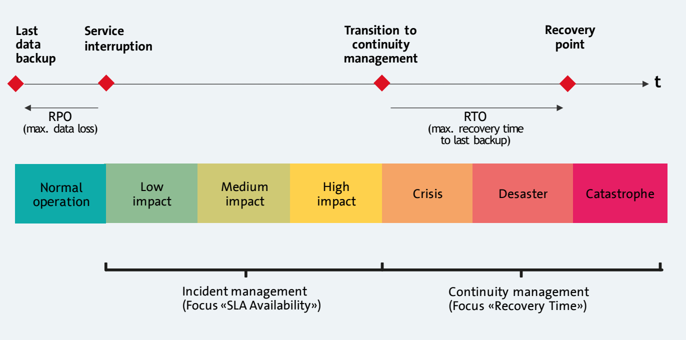

Requirements:
IT Security Levels
– Individual security needs (solution not part of the service portfolio)
– Additional security needs (solution out of the service portfolio)
– Elementary security needs (included as standard in the services)
IT Security Level Customized (ITSLC)
Security Level Advanced (ITSLA)
Security Level Basic (ITSLB)

3.7. SSLP Continuity

The «SSLP Continuity» parameter defines the maximum recovery time and maximum data loss after the transition from incident management to continuity management.

Swisscom distinguishes between internal business continuity management and the service and ICT business continuity described in this document.

The following diagram illustrates the aforementioned transition:


Last data backup
Service interruption
Transition to continuity management
Recovery point
t
RPO (max. data loss)
RTO (max. recovery time to last backup)
Normal operation
Low impact
Medium impact
High impact
Crisis
Desaster
Catastrophe
Incident management (Focus «SLA Availability»)
Continuity management (Focus «Recovery Time»)

The decision for the transition can be made by both the customer and Swisscom, depending on the criticality of the situation. A crisis for Swisscom is a sudden extraordinary event with an impact on the reputation, freedom of action or existence of Swisscom. The management of such an event requires coordinated, horizontally and vertically networked, extraordinary measures, as the normal organisational structure, decision-making channels and resources are no longer adequate. Thus, a crisis for the customer does not yet mean a crisis for Swisscom by definition.

The following conditions must be met for the transition to Continuity Management:

1. Swisscom can no longer provide the service (even with a Workaround), and
2. The agreed Service Levels have been breached (and responsibility lies with Swisscom), and
3. No solution to the fault is foreseeable

Swisscom distinguishes between the following three types of continuity, which can be offered depending on the service:

- **ICT Service Continuity (ICTSC)**

  ICTSC comprises supplementary measures, e.g. additional HW/SW/geo-redundancy, and/or procedural measures for a specific service. ICTSC aims to ensure the restoration of a service within the contractually agreed times (Service Level Metrics RTO/RPO) in the event of a crisis. For services that offer a Recovery Time Objective (RTO) or Recovery Point Objective (RPO) with defined Target Values, ICTSC includes regular ICT Service Continuity tests of the service platform. The focus of the continuity test is only on the service platform and not on any peripheral systems that may be affected by the test (e.g. network, identity and access management) or dedicated customer instances. ICT Service Continuity tests are conducted regularly.

  Customer instances can be secured by the additional «ICT Business Continuity» service.
- **ICT Business Continuity (ICTBC)**

  The characteristics of the ICT business continuity solutions are determined on the basis of the customer's needs, the contractual situation and the system complexity.

  The service includes the execution of an ICT business continuity test, the technical review of Swisscom, preparation of the internal recovery plans according to the recovery level and the updating of the alarm organisation.
- **Business Continuity Management**

  Responsibility for Customer-side Business Continuity Management lies with the Customer. Swisscom can support Customer-side Business Continuity Management with individualised and separately agreed ICT solutions that meet the Customer’s BC requirements through appropriate ICTBC and/or ICTSC configurations.

The following Service Levels are used to specify the quality promise regarding continuity:

- The **Recovery Time Objective (RTO)** determines the agreed maximum permissible amount of time needed to recover a service delivered to the Customer after the transition to continuity management.

  The RTO is expressed as the maximum number of hours from the moment of the transition to continuity management.
- The **Recovery Point Objective (RPO)** defines the furthest point in the past to which a system is consistently restored after it has been recovered. Depending on the requirements, recovery mechanisms such as backup, mirroring, etc. may be used for this purpose.

  The RPO is expressed as the maximum number of hours calculated back from the moment the event occurred.

SSLP Continuity	RTO [h] RPO [h]
Metrik	RTO [h:m, BD] = «Recovery Time of the ICT service» time stamp - «Transition to Continuity Management» time stamp
	RPO [h:m, BD] = «Fault» time stamp - «Last Data Backup» time stamp
Example values[1]	RTO 4 h; RPO Near 0

ICT Business Continuity (ICTBC) is defined in the service description of the corresponding Swisscom service.

Support for Continuity Management is available Mo-Su 00:00-24:00.

4. Service Level Reporting

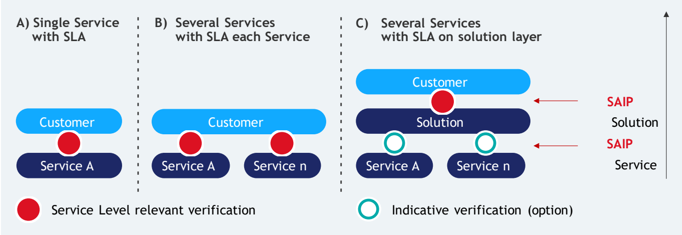
In accordance with the provisions in the individual contract, Swisscom provides standard Service Level Reports as proof of the quality of the standard services. These reports are based on the reporting period and are generally made available electronically.

Individual evaluations - conducted after prior clarification of the feasibility of the Customer’s requirements - can be offered through supplementary services subject to charge, as well as with other reporting periods.

5. Combinations of services

A Customer Solution usually consists of several services, each of which guarantees its respective Service Level promise. The services and the corresponding Service Level promises are combined in accordance with the Customer’s requirements regarding the quality of the customer solution.

The following simplified graphic shows possible combinations of Service Level promises.


A) Single Service with SLA
B) Several Services with SLA each Service
C) Several Services with SLA on solution layer
Customer
Service A
Customer
Service A
Service n
Customer
Solution
Service A
Service n
SAIP
Solution
SAIP
Service
Service Level relevant verification
Indicative verification (option)

- A: One service: One Service Level promise
- B: Several services: Each service has its own Service Level promise
- C: Several services with a combined Service Level promise

In order for Swisscom to be able to guarantee the Service Level promise within the framework of service combinations, the following conditions must be met:

- All affected services must be the sole contractual responsibility of Swisscom
- The Support Time for all affected services has the same or a higher Service Level Target Value as per the customer requirements
- The Service Level promises of the individual services satisfy the same or higher Service Level promises, e.g. application and server and database: each service has a service availability of ≥99.9%
- A combined Service Level promise for combined services requires active monitoring and reporting of the overall solution