Als führender Vertrauensdiensteanbieter in Europa ermöglichen wir die innovativsten, digitalen Geschäftsmodelle.

Basisdokument
Vertragsframework
SLA Definitionen
Service Management
Information Security

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

https://trustservices.swisscom.com
E-Mail: msc.support@swisscom.com

1 Inhalt

2 Einführung

Das vorliegende Dokument ist Vertragsbestandteil eines jeden Servicevertrages zwischen der Swisscom Trust Services AG – nachfolgend «STS» - und dem Kunden.
Es beschreibt

- das Vertragsframework zur Leistungserbringung von Signaturdienstleistungen im Zusammenspiel mit der Swisscom (Schweiz) AG und der Swisscom IT Services Finance S.E.,
- die Definitionen und Erläuterungen zu den in den Leistungsbeschreibung genannten SLA Werten,
- die Informationsmanagementprozesse und die
- Grundlagen zur Informationssicherheit.

3 Allgemeines zur Leistungserbringung von Swisscom Trust Services AG

Die Swisscom Gruppe ist Anbieterin von Vertrauensdiensten für elektronische Signaturen in der Schweiz und in der EU: Die Dienste heissen Signing Service und Selected Signing Service.

Swisscom (Schweiz) AG ist in der Schweiz anerkannte Anbieterin von Zertifizierungsdiensten gemäss Bundesgesetz über die elektronische Signatur (ZertES) und Swisscom IT Service Finance S.E. ist in Österreich anerkannte Vertrauensdiensteanbieterin gemäss EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO).

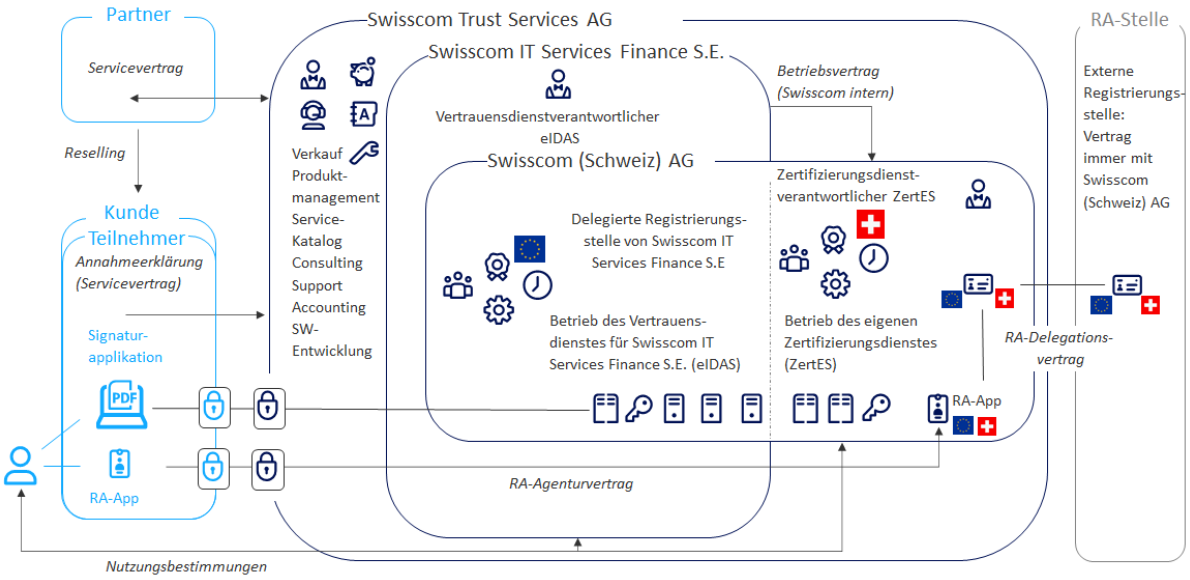
Zertifizierungsdienst und Vertrauensdienst meint grundsätzlich dasselbe, nämlich das Anbieten eines Dienstes für zertifikatsbasierte elektronische Signaturen durch eine "Trusted Third Party". In der Schweizer Rechtsordnung ist von Zertifizierungsdienst und in derjenigen der EU von Vertrauensdienst die Rede.

Der Betrieb des Gesamtsystems für den Vertrauensdienst von Swisscom IT Services Finance S.E. wird technisch von Swisscom (Schweiz) AG auf derselben Infrastruktur in der Schweiz erbracht, auf der Swisscom (Schweiz) AG ihren eigenen Zertifizierungsdienst erbringt.

STS, eine hundertprozentige Tochtergesellschaft von Swisscom, entwickelt und vertreibt die Vertrauensdienste und erbringt damit zusammenhängende Dienstleistungen:

- Weiterentwicklung der Standardmodule zur Fernsignatur und Registrierung
- Gesamtarchitektur des Service
- Produktmanagement und Servicekatalog
- Abrechnung der Servicedienstleistungen
- Abwicklung und Koordination der Inbetriebnahme für den Kunden
- Vertragsabschluss und Kundenkommunikation
- Beratung und Unterstützungsleistungen z.B. im Zusammenhang mit dem Audit

STS vertreibt damit sowohl den Vertrauensdienst nach eIDAS als auch den Zertifizierungsdienst nach ZertES in eigenem Namen und auf eigene Rechnung an Endkunden und Reseller («Kunden»), die wiederum selber diesen Service weiterverkaufen können.



Der Endkunde oder der Reseller («Kunde») schliesst über die Leistungen mit STS einen kommerziellen Servicevertrag ab. Leistungen werden immer gegenüber den sogenannten «Teilnehmer» erbracht. Entweder ist er somit Endkunde von STS oder er hat einen kommerziellen Vertrag mit einem Reseller von Swisscom Services. Sofern der Teilnehmer mit seiner Teilnehmerapplikation Fernsignaturen bezieht, wird die Teilnehmerapplikation Teil des Signaturgesamtsystems und der Teilnehmermuss gegenüber den Vertrauensdiensten die Auflagen an seine Signaturapplikation akzeptieren. Diese Konformitätserklärung gibt der Teilnehmer in Form einer Annahmeerklärung an STS ab, die den Erhalt dieser Erklärung für Swisscom sowohl für den Service nach eIDAS als auch für den Service nach ZertES sicherstellt. Die Teilnehmerapplikation wird Bestandteil des Vertrauensdienstes und unterliegt damit auch den rechtlichen Auflagen und Regularien.

Der Teilnehmer gibt wiederum den Signierenden Zugang zu seiner Teilnehmerapplikation, mit der sie elektronische Signaturen oder Siegel gemäss den Nutzungsbestimmungen von Swisscom erstellen können – jeweils gemäss dem vom Teilnehmer eingesetzten Vertrauensdienst sind es Nutzungsbestimmungen von Swisscom (Schweiz) AG oder von Swisscom IT Services Finance S.E. - und der Teilnehmer stellt dabei im Auftrag des Signierenden die Übertragung der Signaturdaten zum Fernsignaturservice von Swisscom sicher.

Signierende müssen vorgängig entsprechend den einschlägigen Vorschriften über die Vertrauensdienste identifiziert und registriert werden. Diese Identifikationstätigkeit als Registrierungsstelle können Swisscom (Schweiz) AG und Swisscom IT Services Finance S.E. an Dritte delegieren. Im Rahmen der Vertriebsverträge übernimmt STS den Abschluss der hierzu nötigen Verträge mit den Registrierungsstellen im Auftrag und Namen von Swisscom (Schweiz) AG bzw. Swisscom IT Services Finance S.E.. Swisscom (Schweiz) AG kann als delegierte Registrierungsstelle auch für Swisscom IT Services Finance S.E. Delegationsverträge zur Registrierungstellentätigkeit abschliessen.

Neben Projektregistrierungen stehen Standard Registrierungsmöglichkeiten mit ausgewählten Dritten dem Signierenden über den Smart Registration Service zur Verfügung, dessen Auswahl und Kommunikationsmodul entweder von Swisscom oder einem Teilnehmer betrieben wird. Die Applikation stellt sicher, dass die gewünschte Registrierungsmethode ausgewählt wird und der Signierende zum gewünschten Identifizierungspartner weitergeleitet wird.

Darüber hinaus ist Swisscom (Schweiz) AG auch externe Registrierungsstelle der Swisscom IT Services Finance S.E.. Die von Swisscom (Schweiz) AG herausgegebene RA-App kann somit für Registrierungen für beide Vertrauensdienste eingesetzt werden. Einen zugehörigen RA-Agenturvertrag schliessen die Nutzer der RA-App mit STS ab, die den Abschluss im Namen der Swisscom (Schweiz) AG durchführt.

Technisch sind die Systeme des Teilnehmers oder Kunden direkt an die Systeme der Swisscom (Schweiz) AG über eine Schnittstelle gekoppelt. Daher sind sowohl bei der IT Security als auch bei den Service Management Prozessen die Prozesse der Swisscom (Schweiz) AG massgeblich.
Sofern nicht genau zwischen den Swisscom Gesellschaften in den Leistungsbeschreibungen unterschieden werden muss, wird für die bessere Darstellung der Begriff «Swisscom» gewählt. Kommerziell und vertraglich verantwortlich ist die Swisscom Trust Services AG für die Leistungserbringung gemäss den Leistungsbeschreibungen.

4 SLAs

4.1 Übersicht

In den Kapiteln 4-9 werden die Grundsätze der Leistungserbringung, die SLA-Varianten und die verwendeten Standard Service Level Parameter für die Qualitätsdefinition der Services sowie die Service Management Prozesse und IT Security Grundsätze von STS fixiert. Sie bilden die Basis für die Service Level in den Leistungsbeschreibungen und in den Verträgen, die Steuerung während der Leistungserbringung und den abschliessenden Leistungsnachweis (Service Level Reporting).

4.2 Services von STS

Je Service wird in der Leistungsbeschreibung festgelegt, welche Leistungen, KPIs und Zielwerte angeboten werden.

Für jeden Service werden in der Leistungsbeschreibung im Vertrag die folgenden Punkte definiert:

- die angebotenen KPIs und Zielwerte welche die unterschiedlichen qualitativen Anforderungen an einen Service Access Interface Point (SAIP) darstellen;
- die Messverfahren, welche zur Überprüfung der Einhaltung der Service Level Parameters dienen;
- den Standard Service Level Report, welcher die periodische Auswertung der vereinbarten Service Levels zum Nachweis der durch STS erbrachten Leistungen belegt.

Diese Punkte bilden die Basis für das Leistungsversprechen und für den Nachweis der erbrachten Leistungsqualität im Service Level Reporting.

5 Service Level Definitionen

5.1 Best Effort

Das bedeutet, dass sich STS in angemessener und branchenüblicher Weise mit den ihr zur Verfügung stehenden Ressourcen um die Leistungserbringung bzw. Störungsbehebung bemüht, ohne jedoch eine Zusicherung abzugeben. Der Kunde kann Störungen über den Standard *Incident* Prozess melden. Falls kein *Service Level Target* festgelegt ist, gilt die Qualitätsdefinition „Best Effort“.
Service Level Leistungen mit dem Zielwert „Best Effort“ werden nicht gemessen und demzufolge auch nicht in einem Service Level Report aufgeführt. Allfällige Ausnahmen sind in der jeweiligen Leistungsbeschreibung festgehalten.

5.2 Zeitzonen

Falls nicht ausdrücklich an entsprechender Stelle festgehalten oder vereinbart, beziehen sich die Zeitangaben auf die Schweizer Zeitzone.

5.3 Feiertagsregelung

Nationale, allgemeine Feiertage in der Schweiz und Feiertage des Kantons Zürich (Sitz der STS): 1. und 2. Januar, Karfreitag, Ostersonntag, Ostermontag, , 1. Mai, Auffahrt, Pfingstsonntag, Pfingstmontag, 1. August, 25. und 26. Dezember.

5.4 Suspend Time

Die „Suspend Time“ ist die Zeitperiode, während der die Störungsbehebung oder das Request Fulfillment ruht und welche nicht in die Service Level Berechnung einbezogen wird. Gründe dafür sind z.B.:

- Serviceausfälle und Request Fulfillment ausserhalb der vereinbarten Support Time.
- Der Ausfall fällt in ein Provider Maintenance Window, in ein kundenspezifisches Maintenance Window oder in einen angekündigten Serviceunterbruch.
- Ursache einer Störung liegt in der Behebung eines externen System-Fehlers oder in einem Unterbruch des Internet, dessen Behebung nicht in die Leistungsverpflichtung von STS fällt.
- STS beweist, dass weder sie noch ihre Hilfspersonen ein Verschulden an der Störung trifft.
- Bei einem Fehlalarm - der Incident wird mit der Begründung „False Alert“ geschlossen.
- Zeitspannen mit reduzierter Leistungsfähigkeit (latency / transmission delay, throughput packet loss), wenn Messungen von STS belegen, dass die vertraglich spezifizierten Werte erreicht worden sind.
- Der Kunde oder durch ihn beigezogene Dritte verfügen über Berechtigungen, welche potenziell die SLA-Einhaltung beeinträchtigen können (namentlich Root-/Admin-Rechte auf den von STS betriebenen Systemen).
- Der Kunde ist im Rahmen seiner Mitwirkungspflichten nicht verfügbar, um die Störungsbehebung durchzuführen, zu unterstützen oder abzuschliessen. Beispielsweise kann der Incident Management Prozess nicht eingehalten werden wegen fehlender Erreichbarkeit/Zutrittsmöglichkeit, kein Ansprechpartner oder Bestätigung des Kunden. Dies gilt insbesondere auch dann, wenn die Angaben zu den Kontaktpersonen des Kunden von diesem nicht aktualisiert worden sind.

- Die Beistellpflichten des Kunden sind nicht erfüllt.
- Während der Entstörung wird der Kunde als Verantwortlicher für den Fehler identifiziert, wie beispielsweise bei:
    - Applikationen, Ausstattungen oder Einrichtungen, welche nicht zum vereinbarten Serviceumfang gehören (dies gilt namentlich auch für vom Kunden beigestellte Betriebsmittel, wie z.B. im Falle von Fehlern in vom Kunden lizenzierter Software) oder Leistungen von Drittprovider, die nicht vertraglich von STS beigezogen wurden.
    - Fehler vor Ort: z.B. Hausinstallation, kundenseitiges Netzwerk, Strom, Kälte, unsachgemässe Behandlung durch Kunden usw.
- Abwesenheit des Kunden/User zu einem vereinbarten Termin.
- Die Verschiebung des Termins seitens Kunde.

6 Service Level Parameter

6.1 Operation Time

Der Parameter „Operation Time“ ist die Zeitperiode, in der alle für die Leistungserbringung relevanten Servicekomponenten in Betrieb stehen, in der Regel sind dies 7 Tage x 24 Stunden, exkl. Maintenance Windows. Die Einhaltung der Operation Time wird nicht rapportiert.

6.2 Maintenance Windows

„Maintenance Windows“ dienen zur Reservation von Zeiträumen für Wartungsaktivitäten seitens STS und Swisscom. Es handelt sich dabei um Zeitabschnitte, welche nur bei konkretem Bedarf genutzt werden. STS ist bestrebt, die notwendigen Serviceunterbrüche so kurz wie möglich zu halten.
STS unterscheidet zwischen:

- Provider Maintenance Windows der STS Datacenter von Swisscom (PMW-DC)
- Service-spezifische Provider Maintenance Windows (PMW)

Bemerkungen:

- Auf Kundenseite sollten während diesen Zeiten keine Wartungsarbeiten geplant werden.
- Während der Wartungsfenster werden grundsätzlich keine Incident Tickets geführt.
- Am Schluss der Wartungsarbeiten werden die Funktionalitäten derjenigen Services durch STS getestet/geprüft, welche in ihrer Verantwortung liegen. Die übrigen Leistungen – ausserhalb der Verantwortung von STS - müssen durch den Kunden getestet werden.

6.3 Provider Maintenance Windows der Swisscom Datacenter

Die „Provider Maintenance Windows“ der Swisscom Datacenter (PMW-DC) dienen zur Reservation von Zeiträumen für Wartungsaktivitäten in den Räumlichkeiten von Swisscom.
In einem Datacenter sind die folgenden drei Arten von Provider Maintenance Windows (PMW) möglich:
PMWs der Swisscom Datacenter (PMW-DC)

Typ	Beschreibung	Reserviertes Zeitfenster	Service Unterbrüche
General	Für Wartungsarbeiten an der DC-Infrastruktur	Pro Jahr - 8 Wochenenden jeweils Sa 18:00 – So 18:00 Uhr	In der Regel keine/kurze Serviceunterbrüche.
Connectivity	Für Wartungsarbeiten am Netzwerk innerhalb der STS/Swisscom-Datacenter von Swisscom.	Pro Jahr - 4 Wochenenden mit je 3 Nächten: Fr 22:00 – Sa 06:00 Uhr und Sa 22:00 – So 07:00 Uhr und So 22:00 – Mo 06:00 Uhr	In der Regel <1 Stunde
Backup	Für Wartungsarbeiten an der Backup-Infrastruktur.	Wöchentlich Mi 14:00-17:00 Uhr	In der Regel kein Serviceunterbruch

Diese Wartungsfenster gelten für alle Leistungen, welche innerhalb der STS Datacenter produziert werden und ergänzen die servicespezifischen Wartungsfenster, sofern in der Leistungsbeschreibung oder im Vertrag nicht anders festgehalten. Sofern der Kunde von Unterbrüchen von mehr als 2 Minuten betroffen sein könnte, werden die geplanten Provider Maintenance Fenster unter

https://trustservices.swisscom.com/service-status
28 Kalendertage im Voraus publiziert.

6.4 Service-spezifische Provider Maintenance Windows

Das *Provider Maintenance Window* der einzelnen Services (PMW-S) dient der Wartung der servicespezifischen Infrastruktur. Sie ist in den *Leistungsbeschreibungen* festgehalten.

Wenn nicht in der *Leistungsbeschreibung* anders festgehalten, erfolgt keine Abstimmung mit dem Kunden. Sofern der Kunde von Unterbrüchen von mehr als 2 Minuten betroffen sein könnte, werden die geplanten Service spezifischen Provider Maintenance Fenster unter
https://trustservices.swisscom.com/service-status
vorab publiziert.

6.5 Emergency System Changes

Im Betrieb ergeben sich in der Praxis - zusätzlich zu den Maintenance Windows oben - für alle Service-Komponenten kurzfristige Bedürfnisse für Emergency System Changes. STS mit seinem Lieferanten Swisscom behält sich das Recht vor, ausserplanmässig dringende Emergency System Changes z.B. Security Patches sofort durchzuführen.
Die Kunden werden - soweit möglich - kurzfristig vor der Ausführung des Change Request über
https://trustservices.swisscom.com/service-status
informiert. Nach der Durchführung eines Emergency System Changes erfolgt eine Abschlussmeldung an den Kunden.

6.6 Monitored Operation Time

Der Parameter „Monitored Operation Time“ definiert die Zeitperiode (von – bis), während der

- STS den Betrieb des Service gemäss SLA bis zum SAIP sicher stellt.
- bei einer Störung qualifiziertes Personal für Interventionen zur Wiederherstellung von Services bereitsteht und daran arbeitet; d.h. während dieser Zeit werden die vertraglich vereinbarten Service Level Zielwerte (Qualität) sichergestellt;
- im *Service Level Reporting* die Service Level relevanten Abweichungen ausgewertet und nachgewiesen werden.

Während dieser Zeit werden ausserdem

- Störungsmeldungen des Kunden über den 1st Level telefonisch entgegengenommen und an das qualifizierte Personal weitergeleitet.
- Ist der Kunde ein STS Reseller, so ist dieser grundsätzlich bei Störungen zu kontaktieren. Er wird diese zu STS weiterleiten, sofern er diese nicht beheben kann.

Der Zeitraum ausserhalb der *Monitored Operation Time* gilt immer als *Suspend Time*.
Feiertage sind von der *Monitored Operation Time* generell ausgeschlossen, ausser bei „Mo-So 00:00-24:00“, welche alle Feiertage mit abdeckt. Abweichungen von dieser Regel werden in der entsprechenden *Leistungsbeschreibung* festgehalten.

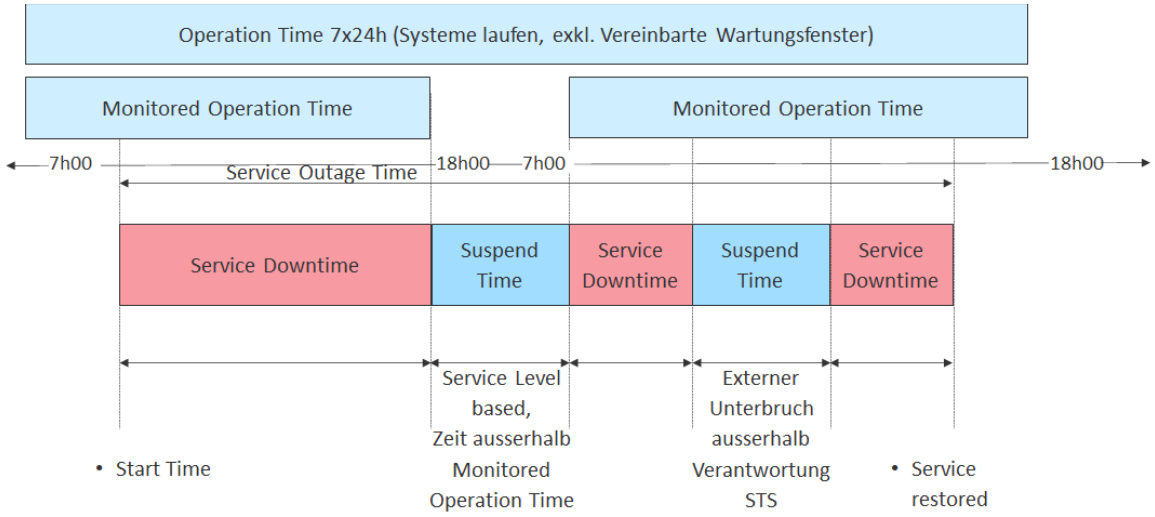
6.7 Support Time

Der Parameter «Support Time » definiert die Zeiten in denen ein qualifizierter 2nd Level Support Kundenanfragen beantwortet und/oder entsprechende kundenspezifische Analysen, Setups und Massnahmen durchführt.

6.8 Availability

Der Parameter „Availability“ bezeichnet die Verfügbarkeit des vertraglich vereinbarten Service am definierten SAIP (Service Access Interface Point). Im aktiven Service Level Management Prozess wird eine Störung einer Service Komponente automatisch erkannt, protokolliert und je nach Monitored Operation Time die Intervention gestartet. Im Incident Management Prozess wird die Zeit einer Störung zwischen „Start Time Stamp“ und „Service restored/wiederhergestellt (Time Stamp)“ erfasst und für den Nachweis „Einhaltung der vereinbarten Verfügbarkeit“ im Service Level Report bereitgestellt (s. nachfolgende Grafik). Workarounds gelten als temporäre Störungsbehebung; wenn der Kunde den Service gemäss Schnittstellbeschreibung am SAIP nutzen kann, gilt er in dieser Zeit als verfügbar.

Die folgende Darstellung zeigt die Relation der verschiedenen Zeiten für den Availability:



6.9 KPI Service Downtime

Der KPI Service Downtime ermittelt die Summe der Service Outage Time [h:m] während der Support Time, exkl. Suspend Time in einer Berichtsperiode. Üblicherweise wird die Service Downtime in h:m als KPI verwendet:

Service Downtime in h:m = Σ Service Outage Time - Σ Suspend Time

6.10 KPI Service Availability

Die Verfügbarkeit als Service Availability wird in % ausgewiesen. Der KPI Service Availability rechnet die aufsummierte Service Downtime [h:m] um in %, in Bezug zur Operation Time während einer Berichtsperiode.

Service Availability in % = (Operation Time - (Σ Service Outage Time - Σ Suspend Time)) / Operation Time×100

6.11 Performance

Der Parameter « Performance » gibt Auskunft über den Status der Auslastung, den Durchsatz, die Messungen und Antwortzeiten von Referenztransaktionen und die Mengen (Aktivitäten, Transaktionen). Für solche Performance-Messungen werden je nach Bedarf bei STS oder im Rechenzentrum von Swisscom ergänzende Techniken wie Probes, Agenten, Recorder und/oder Roboter sowie Monitoring Systeme eingesetzt.
Die Vereinbarung der Messkriterien, des Messverfahrens, der Aufbereitung des Reports und die Konditionen werden in der Leistungsbeschreibung oder im Vertrag geregelt.

7 Incident Management Prozess

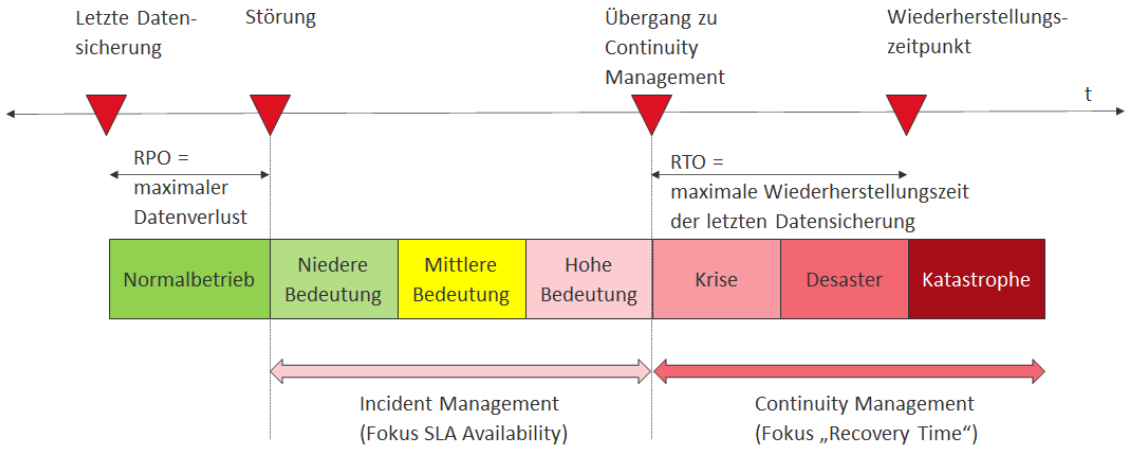
Im Incident Management Prozess werden Störungsmeldungen des Kunden als Incident registriert und ausgewertet. Die Incidententgegennahme erfolgt telefonisch und per E-Mail zu den in der Leistungsbeschreibung genannten Störungsannahmezeiten. Sofern diese übereinstimmen mit der Monitored Operation Time werden telefonisch gemeldete Incidents, die auf einen Ausfall einer Servicekomponente hindeuten dem Personal mitgeteilt, damit ggfs. Systeme restartet oder auf Ersatzbetrieb umgeschaltet werden können.

Während der Support Time werden auch kundenspezifische Incidents bearbeitet und in Kommunikation mit dem Kunden durch Fachpersonal sofern möglich gelöst.

8 Continuity Management

Der Parameter „Continuity“ definiert nach dem Übergang vom Incident Management ins Continuity Management, wie lange maximal die Wiederherstellungszeit dauert und wie gross der maximale Datenverlust ist.

Die folgende Darstellung stellt die verschiedenen Zielwerte im Kontext des Continuity Managements dar:



Der Übergang vom *Incident Management* zum *Continuity Management* ist ein Business-Entscheid (im Weiteren als «Krisenfall» bezeichnet). Diese Entscheidung wird von STS anhand der Auswirkungen auf den Kunden getroffen.

Die folgenden Voraussetzungen müssen für den Übergang ins Continuity Management gegeben sein:

- STS kann die Serviceleistung nicht mehr erbringen (auch nicht mit einem Workaround) und
- die vereinbarten Service Level sind verletzt worden (und die Verantwortung liegt bei STS) und
- es ist keine Lösung der Störung absehbar.

STS unterscheidet zwischen den folgenden drei Arten von Continuity, welche je nach Service angeboten werden können (siehe jeweilige Leistungsbeschreibung):

STS Service Continuity (STSSC): STSSC umfasst ergänzende Funktionen z.B. zusätzliche HW-/SW-/Geo-Redundanz und/oder prozessuale Massnahmen zu einem bestimmten Service. STSSC hat zum Ziel, im Krisenfall die Wiederherstellung eines Service innert vereinbarten Zeiten (KPI RPO/RTO) sicherzustellen.

Customer Business Continuity (BC): Aus Sicht des Kunden hält BC alle Massnahmen fest, die notwendig sind, um den Geschäftsbetrieb umgehend nach einem Krisenfall sicherzustellen. BC beinhaltet alle organisatorischen, personellen und technischen Schritte. Die Massnahmen helfen Kerngeschäfte nach Eintritt des Notfalls schnellstmöglich weiterzuführen, um den Schaden zu minimieren.

Die Verantwortung des kundenseitigen Business Continuity Management liegt beim Kunden. STS kann diesen Prozess mit individualisierten separat vereinbarten Supportleistungen unterstützen.

Zur Spezifikation des Qualitätsversprechens von Continuity werden die folgenden KPIs eingesetzt:

- RTO (Recovery Time Objective) bestimmt die vereinbarte maximale Zeitspanne für die Wiederherstellung eines dem Kunden gelieferten Service nach dem Übergang ins Continuity Management.
  RTO wird in maximal Anzahl Stunden ab dem Zeitpunkt nach dem Übergang ins Continuity Management angegeben.
  RTO [h:m] =
  Time Stamp “Wiederherstellungs-Zeitpunkt des Service” - Time Stamp “Übergang Continuity Management”

- RPO (Recovery Point Objective) definiert den maximal in der Vergangenheit zurückliegende Zeitpunkt, auf den ein System nach dessen Wiederherstellung konsistent wieder aufgesetzt wird. Hierzu kommen je nach Anforderung Wiederherstellungsmechanismen wie Backup, Mirroring usw. zum Einsatz.
  RPO wird maximal Anzahl Stunden - ab dem Ereignis-Zeitpunkt zurückgerechnet - angegeben.
  RPO [h:m] = Time Stamp “Störung” - Time Stamp “Letzte Datensicherung”

Das Continuity Management wird während der Monitored Operation Time erbracht.

9 Service Level Reporting

STS liefert für die Standard Services bei Bedarf und auf explizite Anfrage aufgrund einer gemeldeten Störung einen monatlichen Service Level und Mengen Report als Qualitäts- und Mengennachweis gemäss Definitionen in der Leistungsbeschreibung. Das Standard Reporting basiert auf einer Berichtsperiode von einem Kalendermonat und wird elektronisch zur Verfügung gestellt.

10 Service Management System

10.1 Einleitung

Das Service Management bezeichnet die Gesamtheit von Aufgaben, Massnahmen und Methoden um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT Organisation von STS und Swisscom zu erreichen. Es sichert die Gewährleistung und Überwachung der-Services der für den Kunden sichtbaren Service-Leistungen. Für die Erbringung der Services für unsere Kunden stützt sich STS auf den Service Dienstleister Swisscom (Schweiz) AG und nutzt damit auch ihr Service Management System. Dieses ist ISO 20000 zertifiziert und basiert auf den "Good Practices" von ITIL. Dieses Dokument beschreibt die wichtigsten Prozesse in diesem System und die dazugehörige Governance in Bezug des auf STS erbrachten Service.

Die Einführung neuer und veränderter Services in die Betriebsphase erfolgt gemäss den in diesem System beschriebenen Service Management Prozessen. Neue und geänderte Kundenanforderungen fliessen durch kontrollierte Service Releases in die Leistungserbringung ein.

Der Kunde arbeitet mit seinem Growth Manager, Sales Support bzw. Service Desk zusammen. Ist der Kunde ein STS Reseller, so ist dieser grundsätzlich die erste Anlaufstelle des Teilnehmers. Er wird dann STS kontaktieren, sofern er die Unterstützung von STS bzw. Swisscom benötigt.

STS unterscheidet auf Kundenseite die folgenden Rollen:

Rolle	Funktionen
Sponsor	Auftraggeber von STS
Business Representative	Service Verantwortlicher, der im Kundenvertrag als technischer oder vertraglicher Verantwortlicher genannt wurde
User	Signierende und Mitarbeiter des Kunden, die den Service nutzen
Kunden Service Desk	Kundeninterner Service-/Helpdesk

10.2 Governance

Die Governance zwischen Kunde und STS während der Vertragsphase soll den vereinbarten Servicebezug und die geregelte Serviceveränderung sicherstellen. Dazu bedarf es einer den Bedürfnissen gerechten schlanken Governance-Struktur. Falls nicht anders vereinbart, setzt sich diese aus den nachfolgenden Rollen und Aktivitäten zusammen.
Der konkrete Service und die darin erbrachten und vereinbarten Leistungen sind im Vertrag und den darin vereinbarten Leistungsbeschreibungen definiert.

Rolle	Funktionen	Erreichbarkeit
Growth Manager	Verantwortet die Kundenbeziehung: • Stellt eine optimale Kundenzufriedenheit sicher • Stellt die Gesamtübersicht über die Kundenbeziehung sicher • Stellt eine proaktive Kundenkommunikation sicher (v.a. auf Management Ebene) • Erfasst die Kundenbedürfnisse und -anforderungen • Unterstützt den Kunden bei der Bestellung • Ist die zentrale Anlaufstelle für alle kommerziellen Belange	Bürozeiten Mo-Fr. 8h00-17h00
Sales Support	Stellt im Angebots- und Deliveryprozess die Kundenkommunikation und Abwicklung sicher: • Koordination der Bestellung und Angebote mit Growth Management, Fulfillment, Accounting	Bürozeiten Mo-Fr. 8h00-17h00

	• Sicherstellung aller notwendigen Bestellunterlagen • Bestellbestätigung, Koordination der Unterschriften • Ansprechpartner für Auskünfte rund um Billing, Bestellung und generelle Complaints • Kündigungsmanagement • Entgegennahme und Pflege von Änderungswünschen	
Customer Service Manager	Ist für den Kunden direkter Ansprechpartner für alle Services & Operations Belange: • Ist zuständig für die vertragskonforme Leistungserbringung in der Setup- und Betriebsphase • Ist Anlaufstelle für alle betrieblichen Aspekte des Kunden, welche nicht anders platziert werden können • Ist zuständig für das Service Improvement und identifiziert kontinuierlich Optimierungspotential, definiert Massnahmen und bringt diese zur Umsetzung • Ist verantwortlich für das Service Level Reporting. Überprüft die Güte der vereinbarten Leistungen und leitet wo nötig Verbesserungsmassnahmen ein • Überprüft und kontrolliert die Erbringung von Mitwirkungs- und Beistellpflichten des Kunden und fordert diese bei Bedarf nach	Bürozeiten Mo-Fr. 8h00-17h00
Service Desk	Ist neben Online und E-Mail eine der Schnittstellen zum Kunden für Incident Management (Störungsbearbeitung) und Service Request Management (Bestellungsabruf & Information Request). Die Kontaktinformationen werden im Rahmen des Onboardings festgelegt: • Kategorisiert und klassifiziert Incidents und löst diese, wenn möglich • Weist Incidents bei Bedarf der richtigen Fachstelle zu • Überwacht den Bearbeitungsfortschritt und eskaliert, wenn nötig • Hält den Kunden/User auf dem Laufenden • Schliesst das Ticket nach Wiederherstellung der Services / Bestellungsabschluss • Nimmt Service Requests entgegen, bearbeitet sie und gibt sie an den entsprechenden Stellen weiter	Service Requests und Störungsannahme: Mo-So : 0h00-24h00 Supportzeiten sind in den Leistungs-beschreibungen geregelt
Major Incident Manager	Leitet und koordiniert die Arbeiten zur Behebung von Major Incidents (Störung mit kritischer Auswirkung für den Kunden). Dazu werden Eskalationsmanager/Major Incident Manager bei Kunden und STS alarmiert sowie beteiligte Stellen bei Kunden und STS bzw. Swisscom im Störungsfall koordiniert. Er ist für die Kommunikation während der kritischen Störung verantwortlich: • Nimmt die Störung entgegen und beurteilt diese (allenfalls mit Escalation Manager des Kunden) bezüglich Kritikalität & Störungsbearbeitung • Übernimmt die Koordination mit Kunde auf Stufe Major Incident Management • Führt Telefonkonferenzen, Task Forces und koordiniert die Arbeiten zur Behebung von Major Incidents • Stellt die Information an Kunde/STS auf Stufe Major Incident Management sicher	Bei Eskalationen und Major Incidents Mo-So: 0h00-24h00

10.3 Mitwirkungspflicht und Verantwortlichkeiten des Kunden

Der Kunde ist dafür verantwortlich, dass Informationen über kundenseitige Änderungen bezüglich Konfigurationen, Schnittstellen, Anwendungen und Systeme, welche für die gemeinsame Serviceerbringung relevant sind, präzise und zeitgerecht STS zugänglich gemacht werden, um die vertragsgemässe Serviceerbringung zu ermöglichen.

- Die vereinbarten Schnittstellen und Eingangskanäle bezüglich der Service Management Prozesse sind zu nutzen.
- Der Kunde stellt STS vor Inbetriebnahme und während der Vertragslaufzeit die für die Erbringung der Services notwendigen Ressourcen zur Verfügung:

- Kompetente autorisierte Ansprechpartner für die Einhaltung der gemeinsam vereinbarten Serviceleistung (Namen, Adresse, Funktion, Erreichbarkeit, Telefon, E-Mail inkl. Stellvertreter)
- Die erforderlichen Ressourcen, deren Erreichbarkeit und Mitarbeit
- Eine regelmässig aktualisierte Liste der berechtigten Personen, welche den Service Desk für die vertraglich vereinbarten Leistungen in Anspruch nehmen dürfen, damit STS die Sicherheit und Vertraulichkeit in der Serviceerbringung einhalten kann

11 Prozesse und Funktionen im Service Management

11.1 Customer Relationship Management

Das Customer Relationship Management dient der Pflege der Kundenbeziehung und der Beratung des Kunden für alle Fragen im Zusammenhang mit den von STS angebotenen und gelieferten -Services. Im Zentrum steht die gute und einvernehmliche Beziehung zum Kunden. Dazu dienen neben den regelmässigen Meetings auch die Umfragen zur Kundenzufriedenheit und die Möglichkeit Beschwerden abzusetzen.

Nutzen

- Nachhaltige Service Verbesserung durch frühzeitiges Erkennen der Kundenbedürfnisse.
- Einfaches Beauftragen neuer Service Bedürfnisse über den Growth Manager.
- Sicherstellung der Abdeckung von Kundenbedürfnisse durch geeignete -Services.

11.2 Customer Service Management

Das Customer Service Management fokussiert sich auf die vereinbarungsgemässe und SLA-konforme Erbringung der Services.

Nutzen

- Die Kundenbestellungen sind erfasst, dokumentiert und werden bei der weiteren Gestaltung der Services berücksichtigt.
- Verantwortung für die Einhaltung der notwendigen Service Management Prozesse und Vereinbarungen auf Betriebsebene sind klar zugewiesen.

Voraussetzungen

- Im Vertrag sind die Vereinbarungen zwischen STS und Kunde bezüglich der zu erbringenden Servicequalität geregelt. Die standardisierten Service Levels für die Services sind durch die SLA-Definitionen beschrieben und in der Leistungsbeschreibung des jeweiligen Service definiert.

11.3 Customer Service und SLA Reporting

Das Service Reporting (auf Anfrage im Incidentfall) dient dem zuverlässigen, korrekten und zeitgerechten Nachweis der vereinbarten Servicequalität. Das Service Reporting wird im Rahmen des vertraglich vereinbarten Umfangs auf Basis der massgebenden Leistungsbeschreibungen für den Kunden erbracht.

Nutzen

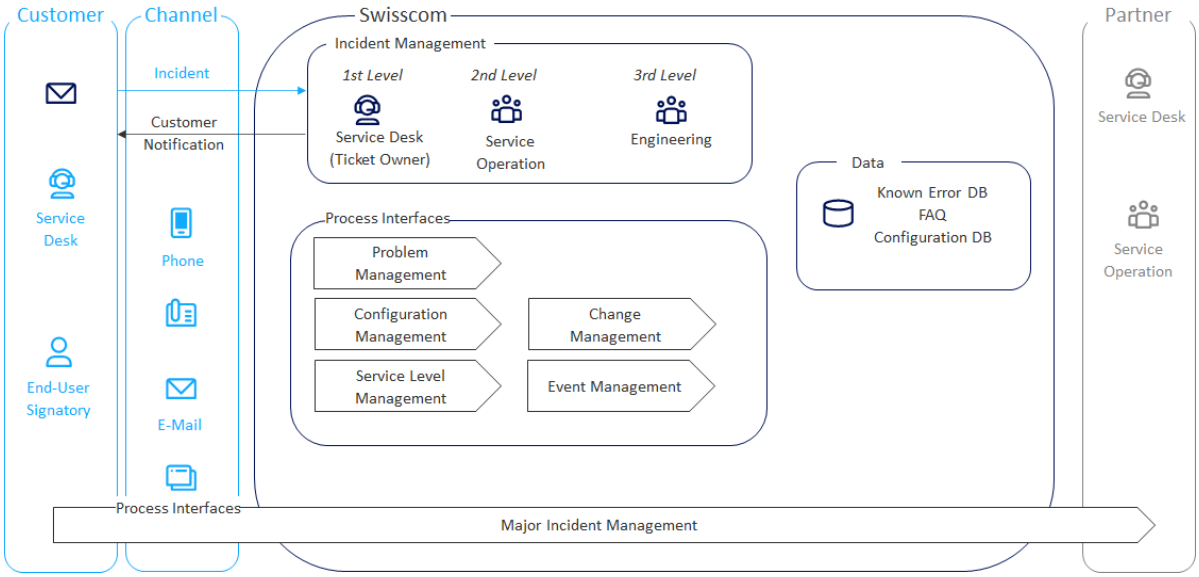
- Nachweis der vertragskonformen Service Erbringung (via Service Level Reporting).
- Report von Service-spezifischen Leistungswerten.

Voraussetzungen

- Keine besonderen Voraussetzungen nötig, Standard Service Reports (SSR) gemäss Leistungsbeschreibung.

11.4 Incident Management

Das Incident Management hat die schnellstmögliche Wiederherstellung der Serviceleistung zum Ziel. Dies erfolgt durch den Einsatz standardisierter Methoden und Prozeduren, bei gleichzeitiger Sicherstellung des Informationsflusses an andere Prozesse, relevante Stakeholder und insbesondere den betroffenen Kunden (reaktiv, wie auch proaktiv).



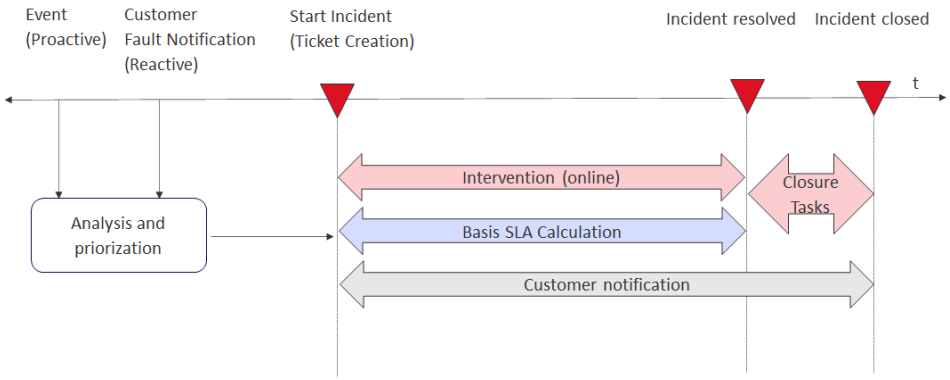
Alle Incidents werden zur Bearbeitung und Nachverfolgung erfasst und nach ihrer Priorität klassifiziert:

Priority	Impact	Beschreibung/Massnahme
Low	Der Incident ist nicht erheblich, kein Einfluss auf die Qualität der Arbeit.	Beseitigung kann geplant und im Rahmen von anderen (Wartungs-) Arbeiten erledigt werden.
Medium	Einzelne oder wenige Benutzer und/oder Geschäftsprozesse sind beeinträchtigt, kurzfristig durch organisatorische Massnahmen überbrückbar.	Intervention gemäss Standard-Prozess (bzw. innerhalb der vertraglich vereinbarten Vorgaben) und regulärer Supervisor Management Unterstützung.
High	Grössere Anzahl von Benutzern und/oder Geschäftsprozessen sind beeinträchtigt, kurzfristig durch organisatorische Massnahmen nicht überbrückbar.	Sofortige (bzw. innerhalb der vertraglich vereinbarten Vorgaben) Intervention durch eine Fachstelle. Aufbietung von anderen Mitarbeitern, die an weniger kritischen Aktivitäten arbeiten (Priority Low oder Medium).
Critical	Unterbruch oder wesentliche Beeinträchtigung von geschäftskritischen Prozessen oder grundsätzliche Störung eines zentralen Services.	Unverzüglicher (bzw. innerhalb der vertraglich vereinbarten Vorgaben) Einsatz aller verfügbaren und notwendigen Ressourcen von STS wie auch Mobilisierung weiterer Partner bis zur Behebung des Incidents. Der Major Incident Management Prozess wird aktiviert.

STS stellt damit die Fehlerbehebung im Rahmen der SLA-Anforderungen sicher.

Die höchste Kategorie von eskalierten Incident ist der Major Incident, der nach einem gesonderten Verfahren behandelt wird. Unabhängig vom Major Incident bietet STS bei für den Kunden gravierenden Störungen sowie bei SLA-Verletzungen einen definierten Eskalationspfad an. Das Senior Management von STS wird dabei situationsgerecht informiert und involviert.

Der Prozess zur Störungsbehebung ist mehrstufig ausgelegt, um immer den richtigen Grad an Expertise einzubinden, bis hin zur Einbindung von Partnern und Lieferanten. Vor-Ort Einsätze werden durch einen flächendeckenden, professionellen Field Service sichergestellt. Das aktive Monitoring der Service Infrastruktur durch STS und Servicedienstleister Swisscom hat die schnellstmögliche Einleitung der Fehlerbehebung, auch ohne vorherige Meldung des Kunden, zum Ziel.



In der Grafik oben ist der zeitliche Ablauf einer Störungsbehebung beispielhaft dargestellt.

11.5 Major Incident Management

Major Incidents sind schwerwiegende Incidents, welche gravierende Unterbrechungen der Geschäftstätigkeiten verursachen und mit höchster Dringlichkeit gelöst werden müssen. Diese werden innerhalb der STS und Swisscom durch dedizierte Major Incident Manager geführt. Der Abschluss eines Major Incidents erfolgt immer im Einvernehmen mit dem Kunden und einer strukturiert aufgearbeiteten Information im Nachgang an den Kunden.

Nutzen

- Schnellstmögliche Service-Wiederherstellung im Major Incident Fall unter Einbezug sämtlicher STS und Swisscom Ressourcen und Eskalationspfade.
- Single-point-of-contact während Major Incidents (Mo-So 00:00-24:00) sowohl gegenüber Kunden wie auch gegenüber internen Stakeholdern.
- Bei einem individuellen Major Incident stehen dedizierte Vertreter seitens Kunde in direktem Kontakt (Mail und/oder Telefon) mit einem Major Incident Manager von STS bzw. Swisscom, der die Störung betreut. Ausserdem erhalten definierte Kontaktpersonen regelmässige, standardisierte Notifikationen per E-Mail und SMS.
- Bei einem Major Incident mit mehreren betroffenen Kunden werden definierte Kontaktpersonen direkt via E-Mail und SMS informiert.
- Nach der Störungsbehebung erhalten die betroffenen Kunden den entsprechenden Abschlussbericht des Major Incidents.

Voraussetzungen

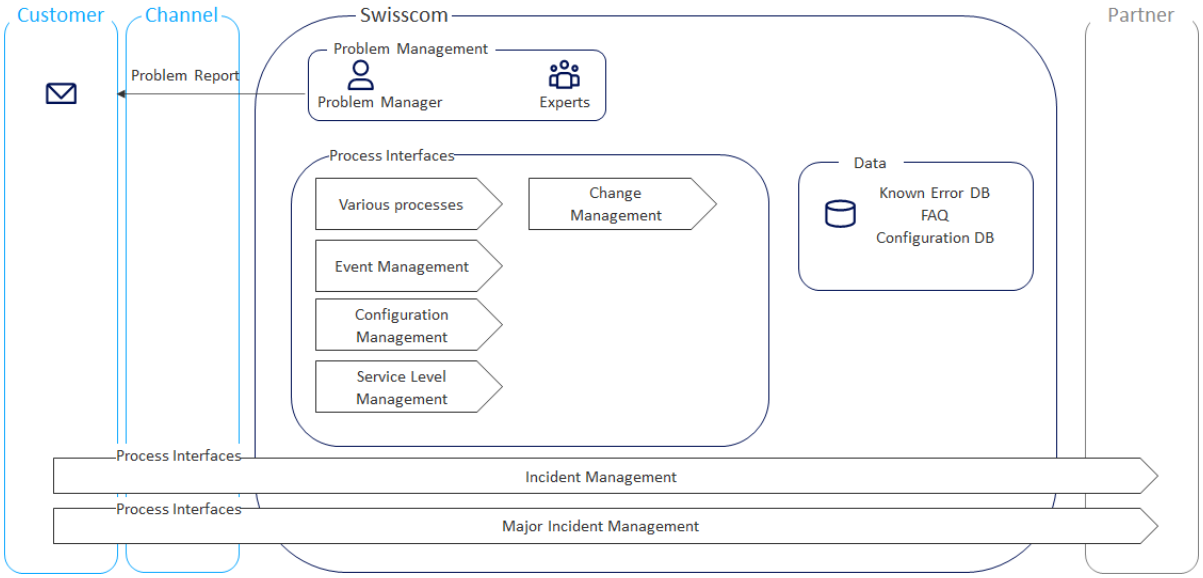
- Entsprechend hoher Business-Impact für Kunden verbunden mit höchster Dringlichkeit (Urgency).

Auswirkung auf die Zusammenarbeit zwischen Kunde und STS

- Der Kunde unterstützt STS bei der Analyse von Störungen.
- Falls Supportaufgaben für Teile der Serviceleistung durch den Kunden selbst erbracht werden, erledigt der Kunde die ihm obliegenden Aufgaben zur Störungsbehebung fristgemäss und informiert STS geeignet über den Stand der Arbeiten.
- Der Kunde stellt eine geeignete Stelle zur Behandlung von Eskalationen bereit, damit STS eine Eskalation in Abstimmung mit dem Kunden in nützlicher Frist bewältigen kann.

11.6 Problem Management

Das Problem Management ist bestrebt, dass nach der Lösung des Incidents (kann auch Workaround sein), die Ursache gefunden und definitiv behoben wird, um künftige Störungen (Incidents) zu verhindern. Problem Management ist eine Disziplin, welche STS üblicherweise ohne direkte Beteiligung des Kunden durchführt. Primäres Ziel des Prozesses ist die Sicherstellung einer nachhaltigen Lösung, bzw. definitive Behebung der Störungsursache zur Vermeidung künftiger diesbezüglicher Incidents.



Nutzen

- Problem Management ist der Prozess, welcher für das Management des Lebenszyklus aller Probleme zuständig ist.
- Wichtigstes Ziel ist deshalb, Anomalien und daraus resultierende Incidents zu verhindern und die Auswirkungen von nicht vermeidbaren Incidents zu minimieren.
- Der Informationsfluss aus und über den Fortschritt des Problem Managements an andere Prozesse sowie relevante Stakeholder ist sichergestellt.
- Nach jedem Major Incident wird der Problem Management Prozess angestossen (per default). Obengenannte Tätigkeiten werden durch das zentrale Problem Management Team sichergestellt.
- Zusätzlich zu den Major Incidents werden ebenfalls Problem Cases mit einer hohen Kritikalität zentral geführt und bearbeitet.

Voraussetzungen

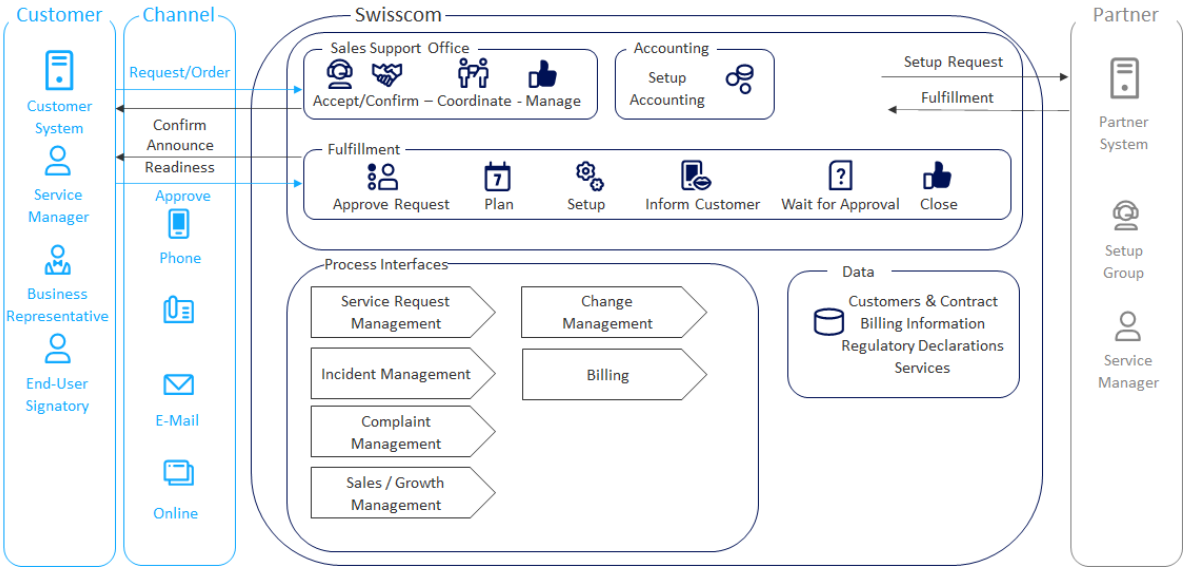
- Abgeschlossene Incidents ohne nachhaltige Lösung mit hoher Kritikalität.
- Abgeschlossene Major Incidents.

Auswirkung auf die Zusammenarbeit zwischen Kunde und STS

- Der Kunde unterstützt STS bei der Analyse von Störungen.
- Falls Massnahmen für Teile der Serviceleistung durch den Kunden selbst erbracht werden, erledigt der Kunde die ihm obliegenden Aufgaben zur nachhaltigen Störungsbehebung selbstständig und informiert STS geeignet über den Stand der Arbeiten und Abklärungen.

11.7 Service Request Management

Der Service Request Management Prozess stellt im Sinne des Request Fulfillment sicher, dass Kundenanfragen und Kundenbestellungen (Orders) über verschiedene Kanäle entgegengenommen, triagiert, bearbeitet und in der vereinbarten Qualität und Zeit ausgeführt werden. Dies beinhaltet auch die Inbetriebnahme und das Auslösen der Fakturierung (Billing). Bearbeitungs- und Ausführungszeiten sind je nach Produkt oder Dienstleistung unterschiedlich und werden mit dem Kunden vertraglich vereinbart.



Service Request Management befasst sich mit folgenden Geschäftsvorfällen

- **Standard Bestellungen (Standard-Order)**: Aus einem vertraglich vereinbarten Katalog abrufbare Produkt und Service Leistungen, z.B. neue Signaturdienstleistungen oder Identifikationsdienstleistungen bestellen, Zugänge bestellen, hinzufügen von Leistungsoptionen, ändern von Leistungsoptionen, Changes, usw.
  Die Standard Bestellung wird in der Regel bearbeitet und auf Vollständigkeit geprüft, beispielsweise kann diese regulatorisch oder vertraglich bedingte unterzeichnete Zusatzdokumente oder Nachweise erfordern. Sofern die Bestellung genehmigt ist, erhält der Kunde die Bestellung mit Vertragsnummer zurückgesendet als Bestellbestätigung. Es kann ein SLA für den Bereitstellungszeitpunkt vereinbart werden abhängig von der Bestellbestätigung.
- **Nicht Standard Bestellungen (Non-Standard Order):** Kundenbestellungen für Hard- und Software, Services oder Changes die komplexer sind und weitere Interaktionen mit dem Kunden benötigen, die sich aber immer noch innerhalb des vereinbarten Customer Service Catalogue befinden. Für die Ausführung braucht es in der Regel eine Koordination oder ein Projekt, welche nach vertraglicher Vereinbarung verrechnet werden.
- **Informationsanfragen (Information Request):** Kundenanfragen irgendwelcher Art, z.B. Rechnungsanfrage, Adressänderung, Auskunft über ein Produkt/Service, Grund einer Störung, Beschwerden, Auskunft über Datenhaltung, etc.

Bestellungen ausserhalb des vertraglich vereinbarten Customer Service Catalogue, Anfragen für Offerten oder auch Incidents gehören nicht zum Service Request Management, d.h. sie werden an die entsprechenden Prozesse (Sales & Fulfillment/Growth Management oder Incident) weitergegeben.

Changes gemäss Change Management Prozess werden über den Service Request Management Prozess angenommen und dem Change-Management Prozess übergeben.

Voraussetzungen

- Für Bestellungen basierend auf Erstbestellungen ist der berechtigte Benutzerkreis (vertraglicher und technischer Kontakt) vom Kunden bekanntzugeben, da nur speziell berechtigte Benutzer Bestellungen auslösen können.
- Entsprechend der vereinbarten kundenseitigen Genehmigungsverfahren für Bestellungen oder Changes stellt der Kunde die Genehmigungsinstanzen und stellt sicher, dass Genehmigungen zeitgerecht durchgeführt werden. Der vertraglich vereinbarte Service Level kommt ab der Genehmigung zur Anwendung.
- Der Kunde nutzt die in den Bestellformularen und Verträgen genannten Kontakte als entsprechende Eingangskanäle für die Service Requests.
- Der Kunde unterstützt STS bei allfälligen Rückfragen zu seinen Service Requests.
- Für die Serviceschnittstelle stellt der Kunde alle nötigen Informationen für die Anbindung der Systeme sicher.

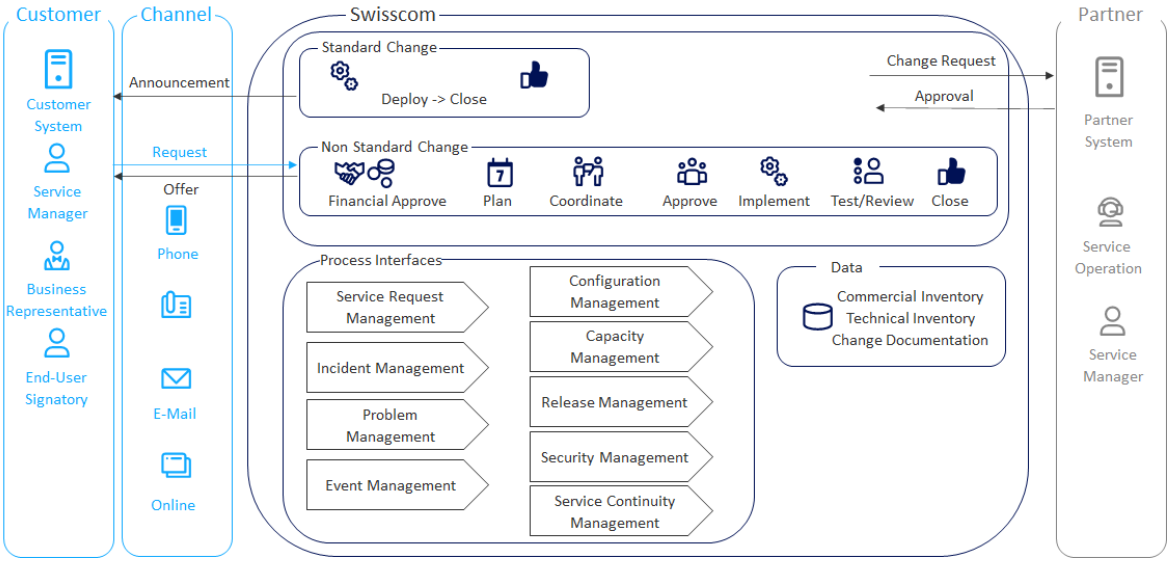
Nutzen

- Effiziente Bearbeitung und Ausführung der Bestellungen zur Zufriedenheit des Kunden unter Einhaltung der vertraglichen Vereinbarungen.
- Sicherstellen der Verrechnung von Bestellungen gemäss vertraglichen Vereinbarungen.

11.8 Change Management

Der Change Management Prozess dient dazu, dass technische Änderungen geplant, kontrolliert und den Anforderungen entsprechend durchgeführt werden. Ziel ist es Änderungen wirtschaftlich und mit kontrollierten Risiken unter Verwendung standardisierter Methoden und Verfahren auszuführen. Der Prozess stellt den Informationsfluss zu anderen Service Management Prozessen und den Stakeholdern sicher (z.B. Kunde, Betrieb, Reseller).

In Situationen wie z.B. Major Incidents, die eine kurzfristige Änderung zur Widerherstellung der Serviceleistung erfordern, kann ein Emergency Change mit verkürzten Prüf- und Freigabeverfahren durchgeführt werden.



Nutzen

- Den geplanten Nutzen eines Changes anforderungsgerecht und wirtschaftlich bereitstellen.
- Erhöhung der Betriebsstabilität durch Minimierung ungeplanter Services und Business Beeinträchtigungen.
- Identifikation von Risiken in der Change Ausführung und Definition geeigneter Massnahmen zur Risikominimierung.
- Dokumentation von Änderungen zur Einhaltung von regulatorischen Vorgaben (z.B. eIDAS, ZertES, ETSI).
- Reduzierung von geplanten Services und Business Beeinträchtigungen durch Nutzung von vereinbarten Change Windows und der Bündelung von Changes.

Changes werden anhand des Risikos kategorisiert und anhand der Dringlichkeit priorisiert.

Das Freigabeverfahren richtet sich nach dem ermittelten Risk Level eines Changes:

Risk Level	Beschreibung des Risikos	Freigabe
1	Standard Change, mögliche Auswirkungen auf einzelne User. Kein geplanter Service Unterbruch.	Pre-Approved
2	Geringes Risiko. Mögliche Auswirkungen auf mehr als einen Kundenstandort und/oder Service. Kein geplanter Service Unterbruch.	Change Manager
3	Mittleres Risiko. Mögliche Auswirkungen auf viele Standorte und/oder Services weniger Kunden. Geplanter Service Unterbruch.	Change Advisory Board (CAB)
4	Grosses Risiko. Mögliche Auswirkungen auf viele Kundenstandorte und/oder Services vieler Kunden. Geplanter Service Unterbruch.	Management Board (BL)

Voraussetzung:

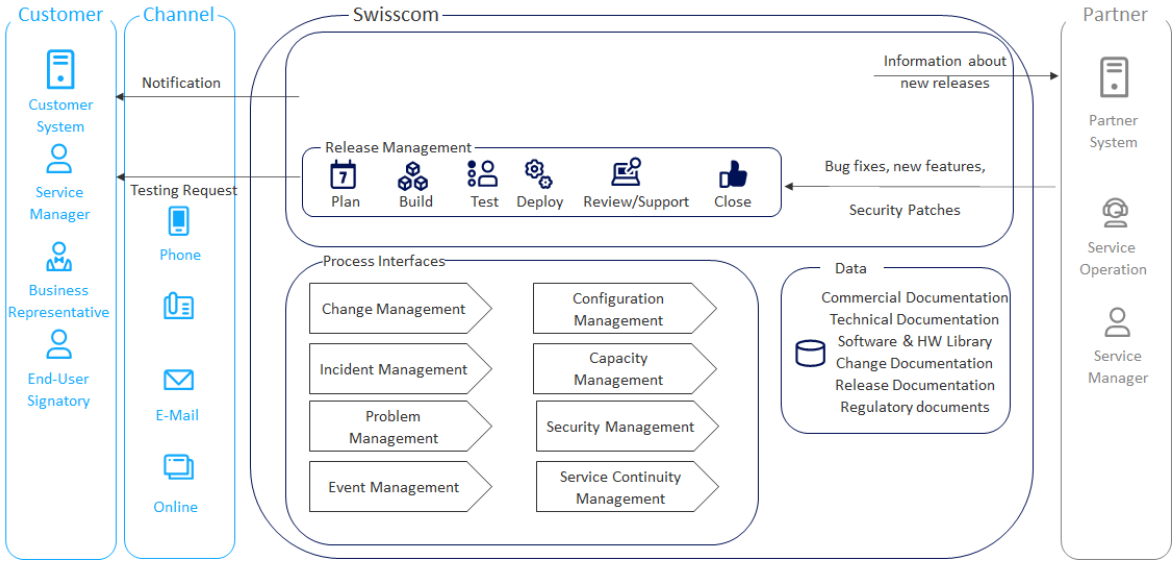
- Alle Änderungen an operativen Systemen bedingen einen dokumentierten und genehmigten Request for Change (RFC).
- Changes werden nach Möglichkeit nur in den vertraglich vereinbarten Zeiten durchgeführt. Siehe hierzu auch die im Kapitel Release&Deploy Management beschriebenen Provider Maintenance Windows (PMW).

- Entsprechend der vereinbarten kundenseitigen Informations- und Freigabeverfahren für Changes wird der Kunde über Changes auf der Service-Status Webseite informiert.
- Der Kunde ist dafür verantwortlich, dass Changes, Releases und Wartungsfenster von STS auf Kundenseite geplant, genehmigt und zur Ausführung freigegeben werden.
- STS wird über alle kundenseitigen Changes mit potenziellen Auswirkungen auf die Serviceleistung mit ausreichendem Vorlauf informiert.
- Der Kunde muss die Service Status Seite abonnieren, um eine Benachrichtigung hierüber zu erhalten.
- Für geplante Änderungen und Wartungsarbeiten stellt der Kunde auf Anfrage Testpersonen für Abnahmetests nach der Change Implementierung bereit.

11.9 Release & Deployment Management

Ziel des Release & Deployment Managements (RDM) ist es die Stabilität und Integrität der-Services sicher zu stellen, indem nur getestete Komponenten ausgerollt werden. RDM sorgt für die strukturierte Durchführung der Planung, der Entwicklung, des Testings, der Vorbereitung des Deployments, der Verteilung und des Supports nach dem Go Live von Änderungen an Services und Infrastruktur.

Neue Releases dienen dem zeitnahen Beheben von Defekten und Security Issues sowie der Bereitstellung und dem Phase-Out von Features und Services). Releases umfassen die zugehörige Hardware, Software, Dokumentationen und Konfigurationen.



Nutzen

- Änderungen schnell, wirtschaftlich geplant und mit minimierten Risiken bereitstellen.
- Sicherstellen, dass neue oder geänderte Services den erwünschten Business Value in der Anwendung durch die Kunden und Benutzer erzielen können.
- Konsistenz der Service Entwicklung durch Berücksichtigung und Einbeziehung aller Komponenten und aller Stakeholder in den Release Prozess.
- Erhöhung der Betriebsstabilität durch geplantes Patching, Testing und Support nach Release Deployments.
- Planungssicherheit für den Kunden.

Provider Maintenance Window

STS hat mit seinem Dienstleister Swisscom für die Wartung und Instandhaltung der Service-Infrastruktur „Provider Maintenance Windows“ (PMWs) definiert, in denen die notwendigen Arbeiten an der Infrastruktur ausgeführt werden. In Absprache mit dem Kunden kann STS weitere spezifische Wartungsfenster definieren, welche für unkritische Arbeiten auch während der Bürozeiten liegen können. Detaillierte Angaben zu den verschiedenen PMWs befinden sich weiter oben in den SLA-Definitionen. Weiteres regelt die jeweilige Leistungsbeschreibung der jeweiligen Services.

Emergency oder Critical Patches

In dringenden Fällen (Critical Patch Management), wenn die Verfügbarkeit oder die Sicherheit der Services beeinträchtigt ist, wird STS präventive Wartungen durchführen. Diese finden nach Möglichkeit innerhalb des PMWs statt und werden via Service Status Seite bzw. den benannten Ansprechpartnern des Kunden, wenn immer möglich, im Voraus gemeldet.

Kundenseitige Wartungsarbeiten

Plant der Kunde Arbeiten, z.B. auch Massentests, bei welchen die lokale „on premise“ Service-Infrastruktur von STS betroffen ist, muss der Kunde diese vorgängig an STS melden. Werden Wartungsarbeiten nicht gemeldet, reagiert die Überwachung der Service-Infrastruktur und der Incident Management Prozess wird angestossen. STS behält sich vor, die entstehenden Kosten in Rechnung zu stellen.

Frozen Zones

Frozen Zones sind im Voraus definierte, kommunizierte Zeitperioden, in denen keine geplanten Wartungsarbeiten, Changes und Releases ausgeführt werden - ausgenommen sind kurzfristig notwendige Changes zur Störungsbehebung. Frozen Zones sind im Interesse der Kunden definiert, um Ihre Businessprozesse während wichtiger Abschlussphasen nicht zu beeinträchtigen. Frozen Zones sind auf Quartalsenden, im Speziellen auf das Jahresende geplant. Die genauen Zeiten und weitere Einzelheiten zu Frozen Zones werden durch den Customer Service Manager abgestimmt und dem Kunden mitgeteilt, sofern für den Kunden relevant.

11.10 Demand & Capacity Management

Das Hauptziel des Demand & Capacity Management ist es sicherzustellen, dass jederzeit ausreichende Kapazität zur Verfügung steht.

Nutzen

- Basierend auf den Forecasts oder aufgrund konkreter Bestellungen werden von STS im Rahmen des Capacity Managements ausreichend Ressourcen zur Verfügung gestellt, damit der Service gemäss SLA erfüllt werden kann.

Voraussetzungen

- Der Kunde unterstützt STS mit den notwendigen Informationen bei der proaktiven Kapazitäts- und Verfügbarkeitsplanung bei Inbetriebnahme und während der Betriebsphase.
- Die vom Kunden aufgenommenen Bedürfnisse und Entwicklungen fliessen in den Capacity Management Plan mit ein.

11.11 Access Management

Access Management koordiniert die Rechtevergabe für Zugriffe auf -Services durch autorisierte Benutzer und verhindert unberechtigte Zugriffe. Im Rahmen des hier beschriebenen Access Managements wird auf den Zugriff des Kunden auf Systeme/Applikationen von STS fokussiert. Der Kunde hat grundsätzlich keinen Access auf die Infrastruktur von STS bzw. Swisscom.

Der Kunde bekommt in der Regel Zugang auf die Serviceschnittstellen über dedizierte Serviceaccounts.

Der Kunde bekommt ggfs. ebenfalls Zugriff auf die benötigten Collaborations Plattformen, z.B. Self-Service Portale, Ablagen, etc. Hier gilt, dass die dafür anzulegenden Benutzerkonten, Rollen und Berechtigungen in der Verantwortung des Kunden liegen.

STS stellt die nötige Infrastruktur zum Anlegen und Verwalten von Benutzerkonten, Rollen und Berechtigungen zur Verfügung.

Die Authentifizierung von Kunden und Kundensystemen auf Services bei wird mittels gängiger Authentifizierungs-Massnahmen z.B. 1- oder 2-Faktor Authentisierung oder zertifikatsgesicherten Zugang sichergestellt und überwacht. Allfällig benötigte physischen Zutritte in die STS bzw. Swisscom Infrastruktur (Gebäude, Rechenzentren etc.) werden aktiv geprüft und überwacht.

Es sind keine regelmässigen Reports im Access Management vorgesehen. Der Customer Service Manager von STS kann auf Anfrage eine Auswertung bzgl. bestehender Gruppen und deren Mitglieder erstellen. Solche Reports sind je nach vertraglichen Vereinbarungen kostenpflichtig.

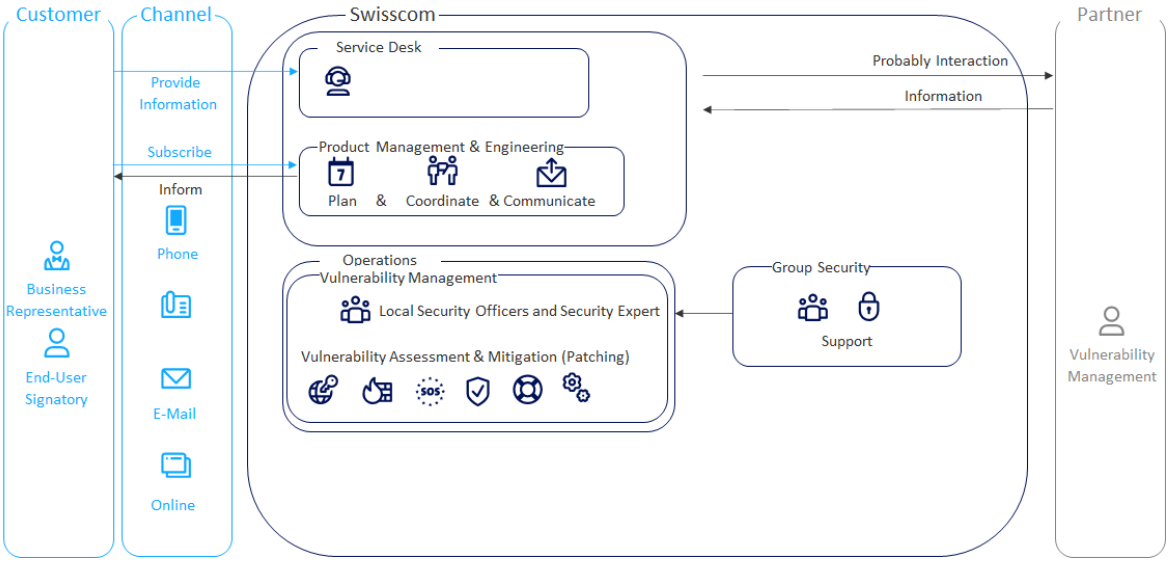
11.12 Service Continuity Management

Der Service Continuity Management Prozess stellt sicher, dass die vertraglich vereinbarten Wiederherstellungszeiten (RTO, RPO) eingehalten werden, um in Krisensituationen die Services entsprechend weiterherzustellen.

11.13 Vulnerability Management

STS erhält von den Herstellern oder anderen Quellen regelmässig Informationen zu Schwachstellen. Diese werden vom Betrieb innerhalb des Vulnerability Managements evaluiert und nach standardisierten Kriterien auf ihren Schweregrad und ihre Auswirkung bewertet. Je nach Schweregrad wird die Behebung der Schwachstelle sofort, in den nächsten Wartungsfenstern oder wie mit dem Kunden vereinbart umgesetzt.

Schwachstellen mit hohem Schweregrad werden zeitnah an die Kunden publiziert. Diese Publikation (auf der Service Status Seite) enthält Informationen zur Schwachstelle, deren Auswirkungen und eingeleitete Massnahmen. STS entscheidet mit seinen Partnern (z.B. Swisscom Group Security) über den Inhalt dieser Kommunikation.
Der Kunde ist seinerseits verpflichtet bekannte Schwachstellen über den Service Desk an STS weiterzuleiten.
Schwachstellen zu bestimmten Produkten und Services, für die es zur Behebung Kundeninteraktionen braucht, z.B. eine Genehmigung des Kunden, werden vom Betrieb über den Customer Service Manager kommuniziert und es wird mit dem Kunden die Umsetzung vereinbart.



Nutzen:

- Schnellstmögliche Behebung von Schwachstellen, die zu betrieblichen Störungen oder Datenverlust führen können.
- Sicherstellung der Verpflichtung, dass sich STS und ihre Kunden bei der Feststellung von drohenden oder bestehenden ICT Security Schwachstellen (Vulnerabilities) gegenseitig umgehend informieren.

Voraussetzungen:

- Die Schwachstellen sind bekannt.
- Der Kunde muss die Service Status Seite abonnieren, um eine Benachrichtigung hierüber zu erhalten.
- Der Kunde verpflichtet sich seinerseits bekannte Schwachstellen über den Customer Service Manager an STS weiterzuleiten.

11.14 Complaint Management

Eine Beschwerde ist eine konkret geäusserte Unzufriedenheit eines Kunden betreffend gelieferte Services oder Dienstleistungen im After-Sales. Das Complaint Management umfasst alle Massnahmen im Fall einer Beschwerde.
Ziel des Complaint Managements ist es die Kundenzufriedenheit trotz eines negativen Erlebnisses aufrechtzuerhalten oder wiederherzustellen. Zudem wird das Feedback des Kunden für das Einleiten von Verbesserungsmassnahmen genutzt, sodass negative Kundenerlebnisse zukünftig vermieden werden.

Nutzen

- Wiederherstellung von Kundenzufriedenheit und Festigung der Kundenbindung.
- Steigerung der Servicequalität durch zügiges Behandeln von Beschwerden und Einleiten von Verbesserungsmassnahmen.
- Reduzierung von Fehler-, Folge- und Beschwerdekosten.

Der Kunde kann direkt über seine Kontaktpersonen (Growth Manager, Sales Support oder den Service Desk) eine Beschwerde bei STS melden. Die Beschwerde wird von einem Complaint Management Team bearbeitet, das mit dem Kunden Kontakt aufnimmt, das Ereignis analysiert und eine schriftliche Stellungnahme für den Kunden verfasst.
Ein Complaint Manager übernimmt im Prozess die Verantwortung für die professionelle und systematische Bearbeitung von Kundenbeschwerden. Er verantwortet die Beantwortung von Kundenbeschwerden in umfassender, zeitnaher Form und in verständlicher Kundensprache.

12 Information Security

12.1 Übersicht

Als Information Security bezeichnet STS Eigenschaften von informationsverarbeitenden und -lagernden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherstellen. Informationssicherheit dient dem angemessenen Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden an den Informationen und der Minimierung von Risiken.

Die IT Security ist eine Teilmenge der Information Security und befasst sich mit der Umsetzung von technischen Massnahmen auf IT Systemen. Neben den technischen Massnahmen gibt es organisatorische und physische Massnahmen um die Information Security zu gewährleisten.

Dieses Kapitel bildet die Basis für die allgemeinen Information Security Aspekte bei Leistungen von STS, die gemeinsam mit Swisscom (Schweiz) AG (nachfolgend «Swisscom») erbracht werden. Es zeigt zudem auf, wie STS im Betrieb die Information Security des Kunden unterstützt. Die Information Security Massnahmen stützen sich insbesondere auf den anerkannten Standard der ISO/IEC 27001, Information Security Management Systems – Anforderung. Swisscom (Schweiz) AG hält dazu seine Zertifizierung nach dem ISO 27001 Standard kontinuierlich aufrecht.

12.2 Informations-Grundschutz Konzept

Die Basis des Informations-Grundschutzkonzeptes von Swisscom bildet ein Grundschutzvorgehen, das gängiger Good Practice entspricht. Die definierten grundlegenden Schutzmechanismen ergeben sich dabei aus grundsätzlichen, allgemeinen Gefährdungen. Auf eine detaillierte Risikoanalyse mit differenzierter Einteilung nach Schadenshöhe und Eintrittswahrscheinlichkeit wird für diese grundlegenden Schutzmechanismen verzichtet.
Das Bedürfnis bezüglich eines Informations-Grundschutzes kann je nach Firma und Tätigkeitsbereich sehr unterschiedlich ausfallen. Aus diesem Grund haben STS und Swisscomeinen mehrstufigen, modularen Informations-Grundschutz festgelegt, dessen Basis-Massnahmen für alle Kunden dieselbe ist.
Diese Basis-Massnahmen werden im Leistungsumfang der Standardservices erbracht.

12.3 Information Security und CP/CPS

Die von STS angebotenen Services sind Dienstleistungen eines auditierten Zertifizierungs- bzw. Vertrauensdienstes. Dieser wird regelmässig auch im Hinblick auf die Einhaltung der Securityvorgaben aus den gesetzlichen Vorgaben und Regularien nach ETSI/CEN geprüft. Die genauen infrastrukturellen, organisatorischen und personellen Sicherheitsvorgaben muss der Zertifizierungs- und Vertrauensdienst daher im Kapitel 5 seiner CP/CPS (Certificate Policy/Certificate Practise Statement) offenlegen. Kapitel 6 der CP/CPS beschreibt die technischen Sicherheitsmassnahmen.

12.4 Grundsätze der Information Security

STS wird im Rahmen der Serviceerbringung Vorkehrungen treffen, damit nur berechtigte Personen Zugriff auf die Systeme erhalten. Zugriffe auf Kundendaten sind nur im Rahmen der mit dem Kunden vereinbarten Leistungen gemäss Leistungsbeschreibung oder anderweitig vertraglich geregelten Fällen erlaubt.
STS überprüft regelmässig, ob die berechtigten Personen mit Zugriff auf die Systeme diese im Rahmen ihrer Aufgabe noch benötigen. Die Berechtigungen werden den veränderten Aufgaben laufend angepasst.
Der Zugriff auf Daten des Kunden erfolgt immer mit starker Authentisierung über ein für solche Zwecke betriebenes Managementsystem.
Die von STS angebotenen Services werden von Swisscom betrieben. Innerhalb von Swisscom wird ein Information Security Management System (ISMS) genutzt, welches eine Aufstellung von Verfahren und Regeln innerhalb von Swisscom ist, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Swisscom orientiert sich am ISO/IEC 27002 Standard, dem ISF Standard of Good Practices, dem BSI IT-Grundschutz-Katalog und ist ISO/IEC 27001 zertifiziert.
Die IT Security Schnittstelle zwischen dem Kunden und Swisscom wird unabhängig von allen übrigen internen IT Security Massnahmen auf Kundenseite im Kapitel „Service Management Prozesse“ im Detail festgelegt. Die Schnittstelle bleibt immer die gleiche, unabhängig davon welche IT Security Levels der Kunde in Anspruch nimmt.
Die Gewalten- und Aufgabentrennung ist ein zentraler Aspekt der IT Security und der Zusammenarbeit. STS und Swisscom haben keinen Einfluss auf die kundeninterne Organisation und Infrastruktur. Die internen organisatorischen Strukturen von Swisscom entsprechen den zertifizierten Normen-Anforderungen. Diese werden durch externe Prüfstellen periodisch auditiert.

12.5 Informationspflichten

STS und der Kunde verpflichten sich gegenseitig zu einer umgehenden Information bei der Feststellung von drohenden oder bestehenden IT Security Lücken sowie der Feststellung von IT Security Incidents, die für die andere Partei von Bedeutung sein können.

12.6 Information Security des Kunden

Der Kunde verfügt über seine eigenen Visionen, Geschäftsstrategien und orientiert sich möglicherweise an Security Standards, welche sich von denjenigen der STS bzw. Swisscom unterscheiden. Anhand von Business Impact- und Risiko Analysen ermittelt der Kunde unter Berücksichtigung der für ihn anwendbaren gesetzlichen und regulatorischen Auflagen die Schutzanforderungen bzw. das gewünschte Schutzbedürfnis. Ebenso ergreift er innerhalb seines Verantwortungsbereichs die zur Wahrung und Aufrechterhaltung des gewünschten Security Levels notwendigen technischen, organisatorischen und physischen Massnahmen und Vorkehrungen.
Sofern er durch seine Applikation Teil eines Fernsignatursystems wird (z.B. Registrierungssystem oder Signaturapplikation) setzt er die von STS ihm genannten regulatorischen und gesetzlichen Vorgaben auch im Hinblick der IT Security um.
Die weitere Verantwortung und Kompetenz zur Bestimmung der Security Anforderungen aus Business-Sicht liegt beim Kunden.
Der Kunde ist dafür verantwortlich, dass seine Mitarbeiter genügend autorisiert sind, um die Schnittstellensystemen zu STS bzw. Swisscom nutzen zu können.
Systeme unter der Verantwortung des Kunden mit technischen Schnittstellen zu STS bzw. Swisscom Systemen müssen gemäss allgemein geltenden „Good Security Practices“ gesichert sein.
Systeme im Eigentum von Swisscom, die beim Kunden vor-Ort installiert werden, müssen vom Kunden entsprechend „Good Practice“ Security Richtlinien platziert werden.

12.7 Datenverarbeitung, Rechenzentren und Infrastruktur

STS verfügt mit seinem Dienstleister Swisscom über eine Rechenzentrumsinfrastruktur, welche auch die Bedürfnisse von Kunden mit sehr hohen Security Anforderungen abdecken kann. Dank einem mehrstufigen Wertschutz-Anlagen-Konzept verfügen die Rechenzentren über einen hohen Security Standard. Durch konsequent georedundante Auslegung der Infrastruktur-Komponenten wird im Rechenzentrum eine hohe Betriebssicherheit und Verfügbarkeit erreicht.

Zutrittsmanagement
Der Zutritt zu Räumlichkeiten, in denen IT Equipment wie Server, Backup Roboter und benötigte Netzwerk-Infrastruktur (z.B. Kommunikation) installiert sind, ist nur berechtigten Personen gestattet und wird mittels physischen Zutrittskontrollen aufgrund angemessener Identifikation und Authentisierung sichergestellt.
Im Detail wurden die folgenden Massnahmen getroffen und umgesetzt:

- Personenvereinzelungsanlagen (Zutritte ins Rechenzentrum nur mit Spezial-Badge und PIN)
- Videoüberwachung der Rechenzentrumszugänge
- 7x24h besetzte Loge in den Rechenzentren-Gebäuden für höchste Sicherheits-Anforderungen
- Rechenzentrum-Zutrittsverfahren mit Badge-Tausch und Identifizierung an der Loge
- Regelmässige Überprüfung der Zutrittsberechtigten durch die zuständigen Asset Owner
- Spezielle Vertraulichkeitsvereinbarungen und Verhaltensanweisungen für Personen mit Rechenzentrum-Zutritt

Mitarbeiter haben nur im Rahmen ihrer definierten Tätigkeit Zutritt zu den Rechenzentren. Die Zutrittsvergabe wird sehr restriktiv gehandhabt. Die Rechenzentrumszutritte sind nicht auf den persönlichen Badges der Mitarbeitenden, sondern auf im Rechenzentrum sicher hinterlegten Spezial-Badges aufgeschaltet.

Infrastrukturversorgung
Im Bereich Infrastrukturversorgung sind ausgedehnte Massnahmen umgesetzt, insbesondere:

- redundante Zuführungen von Versorgungsleitungen und Netzwerkanschlüssen
- USV und Notstromaggregate
- redundante Klimaversorgung

Brand- und Wertschutz
In den Rechenzentren sind Brand- und Wassermelder und eine Brandfrüherkennung installiert. Rauchgas-Detektoren schliessen im Ereignisfall die Luftzuführung. Zur Detektion von Einbruchsaktivitäten sind an den neuralgischen Stellen Wertschutzsensoren platziert.
Bei Brand- und Einbruchsalarmen werden automatisch Alarme an die Interventionskräfte (Feuerwehr bzw. Polizei), das Facility Management und das Rechenzentrum Security Team von Swisscom ausgelöst. Wird Wasser via Fühler in einem Rechenzentrum detektiert, erfolgt ein automatischer Alarm beim Facility Management und beim Rechenzentrum Security Team.

Für die Erstintervention bei einem Brand stehen vor Ort ausreichend dimensionierte Löschwerkzeuge zur Verfügung. Das Personal mit Zutritt zu den Rechenzentren und das Logenpersonal sind in deren Anwendung entsprechend geschult.

Büro- und weitere Produktionsstandorte
STS setzt neben den Rechenzentren auch an allen relevanten Büro- und Produktionsstandorten Verfahren und Infrastruktur ein, welche den grundlegenden Anforderungen an den Informationsschutz gemäss den internen Policies entsprechen. Der Zutritt zu Räumlichkeiten, in denen Daten des Kunden aufbewahrt, offengelegt oder verarbeitet werden, ist nur berechtigten Personen gestattet und wird mittels stetiger Zutrittskontrollen sichergestellt. Mitarbeiter haben nur im Rahmen ihrer definierten Tätigkeit Zutritt zu den Räumen. Die Zutrittsvergabe wird abhängig von der Vertraulichkeit der verarbeiteten Daten restriktiv gehandhabt.

Transporte und Entsorgung
Werden Daten, Informationen oder Datenträger des Kunden durch STS transportiert, ist STS verantwortlich, dass diese jederzeit durch geeignete Massnahmen gegen Verlust und Zugriffe durch nicht Berechtigte geschützt sind. Nicht mehr benötigte Datenträger werden nach einem dokumentierten, sicheren Verfahren gelöscht und entsorgt.

12.8 Adaption

Die in diesem Dokument enthaltenen Grundsätze und Massnahmen werden durch STS und Swisscom im Rahmen des kontinuierlichen Verbesserungsprozesses periodisch überprüft. Sie werden bei Bedarf, veränderten und neuen Anforderungen, Gefahrenlagen oder Gegebenheiten angepasst. STS und Swisscom halten dabei Prozesse, Verfahren und Systeme zur Gewährleistung der IT Security grundsätzlich auf dem aktuellen Stand von Good Practice. Neue Anforderungen seitens des Kunden werden im vertraglich vereinbarten Change Management Verfahren und den entsprechenden Prozessen abgewickelt.

12.9 Periodische Prüfung und Berichterstattung

Prüfung
Die Umsetzung der in diesem Dokument enthaltenen Grundsätze im Bereich des IT-Grundschutzes werden durch den von STS eingesetzten Dienstleister Swisscom im Rahmen der Prüfungen seines internen Kontrollsystems und der Aufrechterhaltung der Zertifizierungen nach dem ISO 27001 Standard (Unterhalt seines Managementsystems) regelmässig überprüft. Swisscom lässt diese Prüfungen durch unabhängige externe Auditoren durchführen. Zusätzlich finden im Rahmen der Signaturgesetzgebung der Schweiz und der EU regelmässige Prüfungen statt.

13 Definitionen

Begriff	Erklärung
1st Level Support	Der *„Service Desk“* nimmt Anfragen oder *Incidents* der *User* oder weiter definierter Anlaufstellen des Kunden entgegen, klassifiziert, priorisiert und versucht diese im Rahmen einer Störmusteranalyse zu lösen. Andernfalls übergibt er die Supportanfragen oder *Incidents* an nachgelagerte Supporteinheiten und koordiniert den weiteren Verlauf der *Lösung*. Dem *1st Level Support* obliegt die Verantwortung für den *Incident* (Ownership) und die Information des Kunden.
2nd Level Support	Dem *„1st Level Support“* nachgelagerte Unterstützungsleistung durch Fachspezialisten im Rahmen des *Incident Management*. Er kommt zur Anwendung, wenn der *1st Level Support* den *Incident* oder die Supportanfrage nicht selber in der verfügbaren Zeit lösen kann.
3rd Level Support	Dem *„2nd Level Support“* nachgelagerte Unterstützungsleistung (STS, Swisscom oder Dritte, z.B. Lieferant) im Rahmen des *Incident* und *Problem* Managements.
Business Continuity Management (BCM)	Der Prozess *„Business Continuity Management“* ist verantwortlich für den Umgang mit Risiken, die zu schwerwiegenden Auswirkungen auf den Geschäftsverlauf führen können. Für den Fall einer Unterbrechung der Geschäftsabläufe werden im BCM-Prozess die Risiken auf ein akzeptables Mass reduziert und eine Planung der Wiederherstellung von *Business-Prozessen* vorgenommen (*BCP*). Das BCM legt die Ziele, den Umfang und die Anforderungen für das IT Service Continuity Management fest.
Business Continuity Plan (BCP)	Ein Plan, der die Schritte definiert, die zur Wiederherstellung von *Business-Prozessen* erforderlich sind. Der Plan identifiziert darüber hinaus die Bedingungen für das Auslösen des Plans, die darin zu berücksichtigenden Mitarbeiter und Organisationen sowie die Kommunikationsmittel. IT Service Continuity Pläne sind ein wesentlicher Bestandteil von *Business Continuity Plänen*. Zu diesen Anforderungen gehören der *Recovery Time Objective* (*RTO*), der *Recovery Point Objective* (*RPO*) und die mindestens erforderlichen *Service Level Targets* für die jeweiligen *Services*.
BSI	Bundesamt für Sicherheit in der Informationstechnik in Deutschland
Capacity Management (Kapazität, Kapazitätsvorhersage)	Dieser Prozess stellt sicher, dass die Kapazität der *Services* (inkl. ICT Infrastruktur) bereitsteht, um die vereinbarten *Service Level Targets* kosten- und zeitgerecht zu erbringen. Das *„Capacity Management“* definiert den Leistungsumfang, die Menge und die Qualität pro Zeiteinheit eines Ressourcentyps (ICT-Komponente oder *Service*), die auf die vereinbarten *Service Level Targets* ausgelegt sein müssen. Die Kapazitätsvorhersage definiert die voraussichtlich benötigte Kapazität zu einem bestimmten Zeitpunkt (Capacity Plan), abgeleitet vom Bedarf.
Change Advisory Board (CAB)	Das *„Change Advisory Board“* ist ein technisches Gremium autorisierter Personen zur Abstimmung und Freigabe von *Request for Changes* (z.B. System *Changes*). Es unterstützt die grundsätzlichen Zielsetzungen des Change Management Prozesses, u.a. die Abstimmungen zwischen den Beteiligten oder Klärung von Risiken.
Closed	Der Status *„Closed“* bedeutet, dass der *Incident* abgeschlossen ist und die Daten für das *Service Level Reporting* sowie die Fakturierung freigegeben sind. Die Wiederherstellung des *Service* und die Kundeninformation erfolgen bereits beim Status *„Resolved“*.
Complaint (Beschwerde), **Complaint Management**	Ein *„Complaint“ (*eine Beschwerde) ist eine konkret geäusserte Unzufriedenheit eines Kunden betreffend gelieferter Services oder Dienstleistungen im After-Sales. Das *„Complaint Management“* adressiert die standardisierte Bearbeitung von Beschwerden und umfasst alle Massnahmen im Fall einer Beschwerde.
CP/CPS	*Certificate Policy/ Certification Practice Statement*, eine rechtlich relevante Dokumentation der Verfahren, die eine Zertifizierungsstelle bei der Ausstellung ihrer Zertifikate anwendet.
eIDAS	**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices n Deutschland auch **IVT** (*elektronische **I**dentifizierung und **V**ertrauensdienste für elektronische **T**ransaktionen*), bezeichnet die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Die Verordnung trat am 17. September 2014 in Kraft und gilt überwiegend seit dem 1. Juli 2016 (Art. 52 der Verordnung).
ETSI	Europäische Institut für Telekommunikationsnormen. ETSI ist eine gemeinnützige Organisation, die von der Europäischen Union als Europäische Organisation für Normung anerkannt

	ist und das Ziel verfolgt, weltweit anwendbare Standards für die Informations- und Kommunikationstechnologien zu schaffen.
Event (Vorfall, Ereignis)	Ein neues Ereignis, welches einen *Incident* auslösen kann. Relevant für die Messung der Interventions- und *Störung*sbehebungszeit ist der Zeitpunkt der Erfassung des *Incidents* durch *STS* im *Ticket* System.
Fehler (Error)	Vom *Swisscom* zu vertretende Abweichung eines Systemverhaltens (als *Incident* / *Störung* oder als *Problem*) von einer vertraglich vereinbarten Spezifikation, die das korrekte Systemverhalten beschreibt. *Swisscom* unterscheidet zwischen *„Fehler“* (*Errors*) und bekannten *Fehlern* (known *Errors*).
Frozen Zone (Sperrzeiten)	*„Frozen Zones“* sind definierte, kommunizierte Zeitperioden, in denen keine geplanten Modifikationen (*Changes*) wie HW- und SW-Installationen, *Updates* oder *Releases* durchgeführt werden, z.B. am Monats- oder Jahresende, bei welchen die Systeme hoch performant und ohne Unterbruch zur Verfügung stehen müssen. *Frozen Zones* Definitionen haben ein grösseres Gewicht als definierte *Wartungs*fenster. Während der *Frozen Zone* darf nichts ohne entsprechende Freigabe umgesetzt werden.
Good Security Practices	Good Security Practices ist eine Sammlung von technischen, organisatorischen und physischen Massnahmen, die einen risikogerechten Schutz der verantworteten digitalen und physikalischen Werte ermöglicht. Dieser Massnahmenkatalog wird regelmässig auf Aktualität überprüft und entsprechend der bestehenden Gefahrenlandschaft angepasst
Incident	Der *„Incident“* ist ein Ereignis, das nicht Teil des standardmässigen Betriebes ist und eine Unterbrechung oder Einschränkung der Servicequalität oder Kundenproduktivität verursacht oder potentiell verursachen kann. Bei der Erfassung der *Incidents* werden zwei Meldearten unterschieden: • „User-driven“: User/Kunde meldet eine Störung via Telefon, E-Mail, Internet online oder Fax. • „System-driven“: Ein System meldet eine Störung und generiert automatisch ein Incident im Ticket System. Auftretende Symptome werden mit einer Zwischenlösung (*Workaround*) oder durch die endgültige Behebung der Ursache eliminiert. Der *User*/Kunde wird vom *Service Desk* über den Entstörungsfortschritt während der *Service*wiederherstellung informiert.
Incident Management	*„Incident Management“* beschreibt den Prozess, der für das Management des Lebenszyklus aller *Incidents* verantwortlich ist. Das *Incident Management* stellt die schnellstmögliche Wiederherstellung des normalen *Service*betriebs und die Minimierung der Auswirkungen auf das Business sicher.
Incident Time to Resolve	*„Incident Time to Resolve“* definiert die vereinbarte Wiederherstellungszeit pro *Incident* (exklusive *Suspend Time)*.
ISMS	Information Security Management System
ISO/IEC 27001	Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
ISO/IEC 20000	Die internationale Norm ISO/IEC 20000 spezifiziert die Anforderungen für das Service Management von Informatik Dienstleistungen
Leistungsbeschreibung	In der *„Leistungsbeschreibung“* ist der einmalige und wiederkehrende Leistungsumfang eines *Service* definiert mit den dazugehörigen möglichen Qualitätsdefinitionen, den *Service Level* Werten, dem *Service Level Reporting* und den Verrechnungsmodellen.
Lösung (Resolution, Restoration)	Massnahmen zur Behebung der zu Grunde liegenden Ursache eines *Incidents* oder *Problems* oder zur Implementierung eines *Workarounds*.
Major Incident	Ein *„Major Incident“* ist eine Kritikalitätsbezeichnung eines *Incident*, bei dem eine erhebliche *Störung* des Betriebs aufgetreten ist. Durch die erhöhten Auswirkungen auf die Serviceerbringung gegenüber dem Kunden, übernimmt ein Major Incident Manager die Steuerung der Behebung. Die Kriterien für die Auslösung eines *Major Incident* sind im Dokument „Service Management Prozesse“ definiert oder werden - wenn abweichend - vertraglich separat vereinbart.
Managed Operation Time	*Managed Operation Time* ist die *Operation Time*, während welcher Personal zur Verfügung steht (auch im Rahmen *Pikett*), welches auf Alarme oder systemrelevante Incidents, die durch den Service Desk mitgeteilt wurden, reagieren kann. Während dieser Zeit wird kein direkter Kundensupport erbracht. Alle Massnahmen dienen dazu die Verfügbarkeit eines

	beeinträchtigten Service wiederherzustellen. Kundensuppport wird während der *Support Time* erbracht. Ausserhalb der Managed Operation Time gelten Service Ausfälle als Suspend Time.
Operation Time	Der *Standard Service Level Parameter* **„***Operation Time"* definiert die Zeitperiode, in der alle für die Leistungserbringung relevanten technischen *Service* Komponenten in Betrieb stehen, in der Regel sind dies Mo-Fr 00:00-24:00, exkl. Swisscom- und kundenseitige Maintenance Windows. *Interventionen* erfolgen jedoch nur während der *Managed Operation Time*.
Option	Eine *„Option"* ist eine ergänzende, vordefinierte, standardisierte Leistung und Preisposition, welche in Kombination zu einem *Service* erbracht wird.
Patch (Fix)	Ein *„Patch"* ist eine Ausbesserung bzw. ein Programmstück, das zur nachträglichen Verbesserung / Korrektur für bereits genutzte Programmteile oder Anwendungen dient (Korrektur eines *Fehlers* zur Sicherstellung des Betriebs). Je nach Dringlichkeit wird unterschieden zwischen Emergency-*Patch*, Fast-*Patch* und Standard-*Patch*.
Performance	Der *Standard Service Level Parameter* **„***Performance"* gibt Auskunft über Nutzung und Leistungsfähigkeit des *Service*. Dies beinhaltet die Messung z.B. den Status der Auslastung, den Durchsatz, die *Antwortzeiten*, die Mengen durch den Einsatz von Probes, Agenten, Rekorder, Roboter und Monitoren.
Pikett (Ausserhalb der Support Time)	*STS* hält sich mit einem Pikettdienst für Arbeitseinsätze und Betriebsunterstützung nach Bedarf ausserhalb der vereinbarten *Support Time* bereit. Der Pikettdienst kann während der *Managed Operation Time* aufgeboten werden.
Problem	Die Ursache für einen oder mehrere Incidents. Zum Zeitpunkt der Erstellung eines Problem Record ist die Ursache in der Regel unbekannt.
Problem Management	Reaktives *Problem* Management stellt sicher, dass nach der *Lösung* des *Incident* (kann auch *Workaround* sein), die Ursache gefunden und definitiv behoben wird. Proaktives *Problem* Management hat zum Ziel, mittels Identifikation und Analyse von Parametern, künftige *Störungen* (*Incidents*) zu verhindern.
Provider Maintenance Windows (PMW)	*„Provider Maintenance Windows"* sind definierte Standard *Wartung*sfenster von STS (-DC für Datacenter-PMWs, -NWK für Connectivity-PMWs, -S für Servicespezifische PMWs). Die *Provider Maintenance Windows* dienen zur Reservation von Zeiträumen für *Wartung*saktivitäten. Während dieser Zeit können Serviceunterbrüche, die als Suspend Time bewertet werden, entstehen. Auf Kundenseite sollten während der *PMW* keine *Wartung*sarbeiten geplant werden.
Ready for Service (RFS)	*„Ready for Service"* definiert das von *STS* bestätigte Datum, an dem eine vertraglich vereinbarte Leistung betriebsbereit sein wird.
Recovery Point Objective (RPO)	*„Recovery Point Objective"* definiert den am weitesten zurückliegenden Zeitpunkt, auf den ein System nach der Wiederherstellung wieder aufgesetzt wird. *RPO* wird in Stunden - ab dem Zeitpunkt der Störungsmeldung zurückgerechnet - angegeben.
Recovery Time Objective (RTO)	*„Recovery Time Objective"* bestimmt die maximal zulässige Zeitspanne für die Wiederherstellung eines *Service* nach dem Übergang ins *Continuity Management*. Der einzuhaltende *Service Level* kann dabei unter den normalen *Service Level Targets* liegen.
Release	Eine Zusammenstellung von Hardware, Software, Dokumentation, Prozessen oder anderen Komponenten, die für die Implementierung eines oder mehrerer genehmigter *Changes* an *Services* erforderlich sind. Die Inhalte jedes *„Release"* werden als eine Einheit verwaltet, getestet und implementiert. Die Umsetzung von *Releases* bedarf einer vertraglichen Vereinbarung.
Release Management	Der Prozess, der für die Planung, den zeitlichen Ablauf und die Steuerung des Übergangs von *Releases* in Test- und Live-Umgebungen verantwortlich ist. Das wichtigste Ziel des *„Release Management"* ist es, sicherzustellen, dass die Integrität der Live-Umgebung aufrechterhalten wird und dass die richtigen Komponenten im *Release* enthalten sind. Das *Release Management* ist Teil des Release & Deployment Management Prozesses.
SAIP (Service Access Interface Point)	Der *Service Access Interface Point (SAIP)* ist der vertraglich vereinbarte, geografische und/oder logische Punkt, an dem ein *Service* dem Leistungsbezüger bereitgestellt, überwacht und die erbrachten *Service Level* ausgewiesen werden. Er wird in den Leistungsbeschreibungen als Standard definiert und die Zielwerte im Vertrag vereinbart. Es wird festgehalten, ob die Leistungen am SAIP direkt für den Kunden oder indirekt über weitere Services von STS erbracht werden. Solange der vereinbarte Service Level eingehalten wird, ist STS frei in der Gestaltung der Art und Weise wie produziert wird.

Sales Support	Zentrale Anlaufstelle von *STS* (Single Point of Contact) für alle Bestellungen, Verträge und Fragen zur Abrechnung und Stand der Aufschaltung eines *Service*. Störungen und Supportanfragen hingegen werden dem *Service Desk* kommuniziert.
Service (Core Service, Support Service)	Ein *„Service"* umfasst die zwischen dem Kunden und *Swisscom* vereinbarte und zu erbringende Leistung (Menge, Qualität, Preis und Zeitdauer). Der *Service* besteht aus Prozess- und/oder ICT-Infrastruktur-Leistungen. Der Leistungsumfang und die Qualität werden vertraglich vereinbart.
Service Desk (Help Desk, Support Desk, Call Center)	Zentrale Anlaufstelle von *STS* (Single Point of Contact „*SPOC*") für Kunden bei *Störungen* und Fragen sowie Support-Leistungen, die mit der Leistungserbringung von *STS* für den Kunden zusammenhängen. Der *„Service Desk"* ist rund um die Uhr (Mo-So 00:00-24:00) erreichbar.
Service Downtime	Die *„Service Downtime"* [h:m] ist - während einer Berichtsperiode - die Summe der *Service Outage Time* [h:m] während der vereinbarten *Support Time*, exkl. *Suspend Time*.
Service Katalog	Der *„Service Katalog"* fokussiert auf die durch den Kunden während der Vertragslaufzeit bestellbaren Positionen, für die in seinem Vertrag erfassten *Services*. Für die gelisteten Positionen ist der Bestellumfang, die Lieferzeit und der Preis definiert. Der Bestellvorgang (Request / Order) kann entweder durch den *Service Desk* oder Online abgewickelt werden. Die Bestellpositionen sind spezifisch zum jeweiligen *Service* und können sowohl abhängig von den gebuchten Optionen wie auch Kunden individuell sein.
Service Level (SL)	Ein *„Service Level"* dient zur Definition, zur Messung und zur Steuerung der Servicequalität sowie beim Erstellen des Nachweises (SL-*Reporting)*. Die Servicequalität wird mit Hilfe mehrerer *Standard Service Level Parameters*, *KPIs* und *Service Level Target Values (SL-Zielwerte)* im Vertrag (SLA) festgelegt.
Service Level Agreement (SLA)	Das *„SLA"* ist ein integrierender Vertragsbestandteil zwischen *STS* und einem Kunden. Das *SLA* beschreibt und regelt die zu erbringenden einmaligen und wiederkehrenden Leistungen in der Qualität gem. *Service Level* Definition und legt die Verantwortlichkeiten von *STS* und des Kunden fest.
Service Outage (Service Ausfall)	Ein *„Service Outage"* ist eine *Service Level* relevante *Störung*.
Service Outage Time (Ausfallzeit, Service-Wiederherstellungszeit, Service Restoration Time, Resolution Time)	Die *„Service Outage Time"* ist die gesamte Zeitspanne währenddessen die *Service Availability* nicht gewährleistet ist. Sie umfasst die Bruttozeit eines *Serviceausfalls*, d.h. unabhängig der vereinbarten *Support Time* und *Suspend Time*.
Sicherheitsvorfall	Ein *„Sicherheitsvorfall"* ist ein Ereignis, das die im Vertrag mit dem Kunden vereinbarten Schutzziele betreffend der Vertraulichkeit, *Verfügbarkeit* oder Integrität verletzt. Typische Beispiele für einen Sicherheitsvorfall sind ein unberechtigter Zugriff auf die Kunden*services* oder Kundendaten oder ein Virenbefall.
Störung	*„Störung"* bedeutet eine vermeintliche Abweichung der erbrachten Leistung des im Vertrag vereinbarten *Service*. Eine *Störung* liegt vor, wenn die erbrachte Leistung nicht der Qualität gemäss Vertrag entspricht. Eine *Störung* wird in einem *Incident Ticket* erfasst, klassifiziert und untersucht. Eine *Störung* kann durch einen *Serviceausfall*, einen *Fehler*, einen Bedienungsfehler durch den *User* oder durch eine andere Ursache entstehen.
Support Time (Bereitschaftszeit; Unterstützungszeit; Supportzeit)	Der Parameter **„***Support Time"* definiert die Zeitperiode, während der bei einer Störung qualifiziertes Personal für direkten Kundensupport zur Verfügung steht. Diese ist abzugrenzen von der *Managed Operation Time*, bei der das qualifizierte Personal den Fokus auf die Aufrechterhaltung der Verfügbarkeit des angebotenen Services legt.
Suspend Time	Im *Incident Management* Process ist die *„Suspend Time"* die Zeitperiode, während der die *Störung*sbehebung ruht und nicht in die *SL*-Berechnung einbezogen wird. Suspendierte Zeiten werden bei der Berechnung der *Ausfallzeit* respektive der *Verfügbarkeit* als nicht *SLA*-relevant klassiert. Gründe sind z.B. Mitwirkungs- & Beistellpflichten des Kunden, ausserhalb *Maintenance Operation Time*, Feiertage, *Fehler*quelle auf Kundenseite, *Provider Maintenance Windows* usw. Im *Service Request* Process ist die Suspend Time die Zeitperiode, während das Request Fulfillment ruht und nicht in die *SL*-Berechnung einbezogen wird.
Swisscom	Swisscom (Schweiz) AG, Dienstleister im Auftrag der Swisscom Trust Services AG, der für die Kunden direkt den Service technisch bereitstellt und APIs (SAIP) zu Kundensystemen technisch zur Verfügung stellt.
Swisscom IT Services Finance S.E.	Tochtergesellschaft des Swisscom Konzerns in Österreich und anerkannter Vertrauensdienstanbieter in der EU.

STS	Swisscom Trust Services AG, Zürich, Schweiz
Ticket	Detailinformationen zu einem *Incident*, einem *Problem*, einem *Change* oder einem *Service Request,* z.B. dokumentiert ein *Incident Ticket* die Informationen eines Lebenszyklus eines einzelnen *Incident*.
User	Anwender, Benutzer, Signierender oder Mitarbeitende des Kunden, welche den *Service* gemäss Vertrag nutzt.
USV	Unterbrechungsfreie Stromversorgung. Diese überbrückt einen Stromausfall in einem RZ bis der mit Diesel betriebene Generator einsatzbereit ist
Vulnerability Management	*„Vulnerability Management"* ist ein Prozess, um festzustellen, ob Vulnerabilities (Schwachstellen) auf der Grundlage des Risikos und der mit der Behebung der Vunerabilities verbundenen Kosten eliminiert, reduziert oder toleriert werden sollen.
Workaround	Not- oder Umgehungslösung mit dem Ziel einen *Incident* rasch zu beseitigen. Der *„Workaround"* (Umgehungslösung) kann eine temporäre Korrektur sein, ermöglicht dem *User* aber die rasche Weiternutzung des *Service*. Die Nutzung des *Service* kann dabei eingeschränkt sein.
ZertES	Das Schweizer Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) (SR 943.03) regelt den rechtlichen Rahmen um digitalen Signaturen, dessen Einsatz, Anbieter, sowie Rechte und Pflichten. Es regelt ausführender die Anforderungen an eine qualifizierte Signatur, um einer eigenhändigen Unterschrift gemäss Obligationenrecht gleichwertig zu sein.