

PR-XXXXX

PR-XXXXX

Procedure

Major Cyber Security Incident – FINMA report procedure

Valid from	September 1 st , 2020	Version 1.00
Issuing Unit	CISO Region CH	
Author	CISO Region CH	
Contact	Björn Fröhlich	
Replaces	N/A	
Original Language	English	
Scope/Recipients	Credit Suisse Group	

Summary

This procedure specifies the process to inform FINMA regarding a major cyber security incident impacting supporting resources for critical functions. FINMA's primary focus is on the critical functions where successful or partially successful cyber attacks would lead to failure or malfunction.

Goal of this procedure is to ensure prompt reporting of such incidents to FINMA with incident reporting content as mandated by FINMA Guidance 05/2020 "Duty to report cyber-attacks pursuant to Article 29 para. 2 FINMASA".

For cyber attacks meeting FINMA severity level, Credit Suisse has to submit a initial criticality assessment within 24 hours and a full report within 72 hours.

PR-XXXXX

History

Version	Date	Author(s)	Changes
1	09 th June 2020	Björn Fröhlich	First Draft
2	01 st July 2020	Björn Fröhlich	Inserted basic available information
3	06 th July 2020	Björn Fröhlich	Inserted Process diagram, CS mapping to FINMA requirements
4	09 th July 2020	Björn Fröhlich	Review of others input, Abbreviations Appendix
5	10 th July 2020	Björn Fröhlich	Final adjustments – ready for review
6	16 th July 2020	Björn Fröhlich	Updated contact list and Task Force
7	23 rd July 2020	Björn Fröhlich	CSIRT changed to official TDR

Contents

1.	Introduction	3
2.	Scope	3
3.	Reporting Timeline	3
4.	Mapping of FINMA severity level to CS severity level	5
5.	Critical Assets.....	5
6.	Reporting process to FINMA.....	6
7.	Reporting Steps	7
8.	FINMA assessment Task Force	8
9.	Teams, Contacts and Roles	8
10.	Legal Entities	11
11.	Maintenance of the document	13
	Appendix 1: 24h report via email to the FINMA Key Account Managers.....	14
	Appendix 2: 72h report via EHP online system from FINMA	15
	Appendix 3: Root Cause Analysis.....	16
	Appendix 4: Abbreviations.....	17

PR-XXXXX

1. Introduction

FINMA published the guidance 05/2020 "Duty to report cyber-attacks pursuant to Article 29 para. 2 FINMASA". FINMA expects the detailed requirements from the guidance on reporting cyber attacks to be implemented by 1 September 2020.

This procedure is focusing on the reporting of cyber attacks meeting the FINMA severity level. Cyber attacks within Credit Suisse are handled as cyber security incident by Threat Detection and Response (TDR) and following the Major Incident Management (MIM) process.

2. Scope

Cyber attacks meeting the criteria for FINMA severity level to be reported, regardless if they are successful or only partially successful. If the cyber attack does not impact the Swiss Financial Market FINMA only needs to be notified.

FINMA has consolidated supervision, therefore all cyber attacks globally within Credit Suisse Group meeting the FINMA severity levels "Medium", "High" or "Severe" (according to Appendix 1 of the circular FINMA guidance 05/2020) are in scope for 24h / 72h reporting to FINMA. For cyber attacks not impacting Swiss critical assets and in jurisdictions where other regulatory reporting requirements exist, FINMA will consider to collaborate with relevant regulators to get further information in addition to the 24h / 72h report.

Primary focus is on the critical functions where cyber attacks would lead to failure or malfunction. Cyber attacks are normally targeted directly at the supporting resources for these critical functions. Supporting resources that are designated as critical assets include personnel, technology infrastructure, information and facilities as well as critical service providers who support the business processes of these critical functions.

This process is an extension of the base Incident Management standard and its underlying processes which is defined here: [IT Standard S-00030 IT Incident Management](#)

3. Reporting Timeline

FINMA expects that the affected supervised institution inform FINMA through the responsible (*Key*) *Account Manager* within 24 hours of detecting such a cyber attack by submitting an initial assessment of its criticality.

The actual report needs to be submitted within 72 hours via the FINMA web-based survey and application platform (EHP).

The 24h / 72h reporting timeline starts when a cyber attack is confirmed and meet FINMA severity criteria "Medium", "High" or "Severe". Reporting deadlines are valid during Swiss working days (Monday until Friday).

Phase	Channel	Description	Timeline
Initial assessment	Email to FINMA Key Account Managers	Reg Affairs notifies FINMA after a confirmed major cyber security incident	First 24 hours
Full Report	EHP survey and application platform	Reg Affairs sends the full report via the FINMA online portal EHP	First 72 hours*
Root Cause Analysis	Email to FINMA	After the incident is resolved Reg Affairs sends the Root Cause Analysis	After Incident closure

PR-XXXXX

*Note: If material changes occur after the 72 hours, a new report needs to be raised towards FINMA. The 72 hours starts again.

The information for the 24 and 72-hour reports depends on the confirmed impact by TDR.

A cyber security incident may be material or significant for reporting to FINMA (i.e. "reportable") if it meets the following FINMA criteria as defined in the guidance:

Severity	Definition	Criteria
Severe	Extensive and prolonged damage to protective goals (availability, integrity, confidentiality) of critical assets present or expected.	<ul style="list-style-type: none"> Availability: critical assets are not available in the medium to long term (failure > 200 % of the RTO) Confidentiality/integrity: sensitive information affected to (almost) full extent Financial implications or damage to the institution's reputation endangering its existence Overcoming the cyber attack requires the activation of the crisis organization (BCM)
High	Protective goals (availability, integrity, confidentiality) of critical assets are substantially damaged or threatened.	<ul style="list-style-type: none"> Availability: critical assets are not available in the medium term (failure >= RTO) Confidentiality/integrity: sensitive information and/or critical information for the business process affected to a large extent Considerable financial implications or damage to the institution's reputation Overcoming the cyber attack requires the engagement of external resources
Medium	Direct harm or threat to the protective goals (availability, integrity, confidentiality) of critical assets.	<ul style="list-style-type: none"> Availability: critical assets are not available in the short term (failure > 50% of the RTO) Confidentiality/integrity: sensitive information substantially 10 affected Perceptible financial implications or damage to the institution's reputation The cyber attacks can be overcome internally with the resources available

PR-XXXXX

4. Mapping of FINMA severity level to CS severity level

Cyber attacks meeting the FINMA severity levels are handled in Credit Suisse according to the cyber security major incidents process as defined by the global incident management. Therefore in scope of the FINMA reporting are cyber security incidents of CS severity level "Critical" and "High" handled according to MIM.

These severity criteria are aligned to [Global Incident Management Process](#) definition for incidents with extensive and widespread impact. Aligning to these existing processes, incident management team can leverage on existing procedures in categorizing, responding to incidents, and leveraging captured data for regulatory reporting.

In the event of critical cyber security related attacks, incident management team follows the [BCM Cyber Incident Response Framework \(BCIRP\)](#) to address mitigation of the effects of cyber security incident and/or recovery from such an incident.

5. Critical Assets

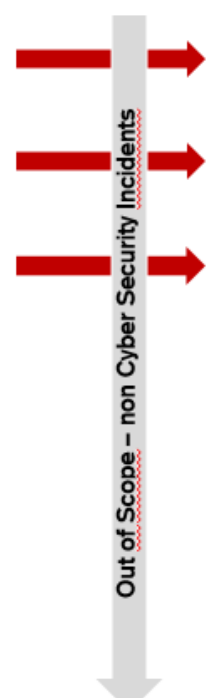
Data of critical functions, corresponding business processes and critical assets are managed in the "OneBCM" tool and governed by BCM. Business processes are registered as "Product, Processes and Activities" (PPA). They contain a Criticality Class (CC1 – CC4) and assets (e.g. personnel, technology, application/ICTO, facilities) are mapped.

ICTOs Criticality Class is available in CATI (see "BCM Criticality Class" – class 1-4). Based on the CS criticality classes and mapping to the FINMA severity levels, ICTOs with rating of "1 – Survivability" and "2 – Significant" are considered as critical and in scope of FINMA reporting.

Critical providers are identified by Sourcing and Vendor Management (SVM) based on regulatory Outsourcing relationships and BCM rating. Data is stored in their inventory "Coupa".

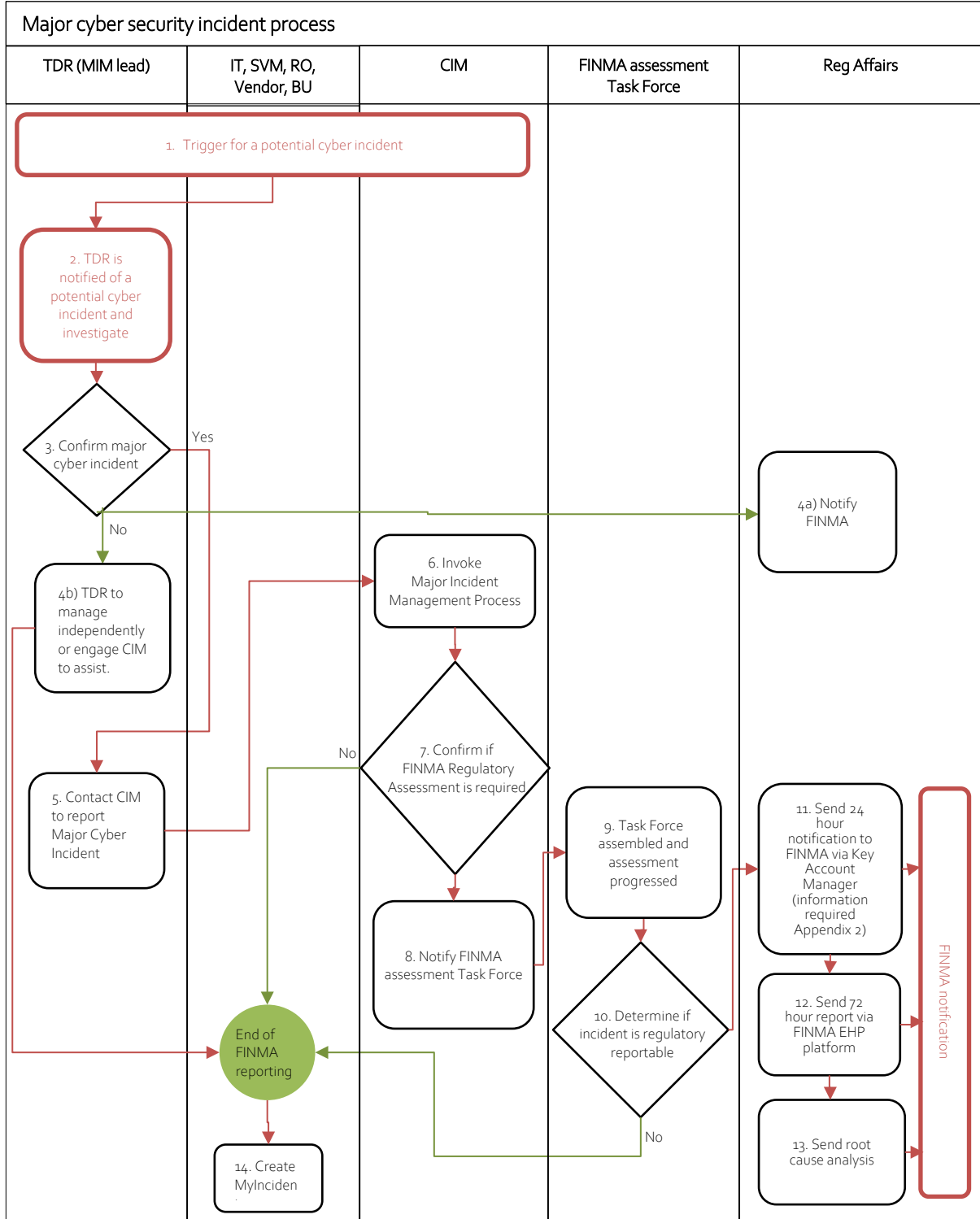
Urgency	Impact (examples)	CS Severity	FINMA Severity
<ul style="list-style-type: none"> Critical: <u>Very urgent: Needs to be solved immediately/now</u> 	<ul style="list-style-type: none"> SLA: <u>Extensive/Widespread SLA breach</u> Financials: <u>Above 100k USD</u> 	Critical	Severe
<ul style="list-style-type: none"> High: <u>Urgent: should be solved as soon as possible</u> 	<ul style="list-style-type: none"> SLA: <u>Significant/Large breach</u> Financials: <u>Less 100k USD</u> 	High (MIM – Impact: Extensive) High (MIM – Impact: Significant) High (non MIM)	High Medium
<ul style="list-style-type: none"> Medium: <u>Little urgency</u> 	<ul style="list-style-type: none"> SLA: <u>Moderate/Limited breach</u> Financials: <u>Less 5k UDS</u> 	Medium	
<ul style="list-style-type: none"> Low: <u>No urgency</u> 	<ul style="list-style-type: none"> SLA: <u>No/minor SLA breach of Non-critical IT assets</u> Financials: <u>No risk of financial impact</u> 	Low	

Out of Scope – non Cyber Security Incidents



PR-XXXXX

6. Reporting process to FINMA



PR-XXXXX

7. Reporting Steps

No.	Activity	Description	Lead
1	Incident reporting	Incident to be reported according to S-00030 IT Incident Standard to TDR	IT / SVM / RO / Vendor / CIM / EUS
2	TDR starts investigation	The Incident will be analyzed by TDR	TDR
3	TDR confirm cyber incident	Decision whether it is a major cyber security incident. If yes, CIM team will be engaged and if necessary TDR will inform the legal team which will contact law enforcement	TDR
4a	Inform FINMA	FINMA notification about any non-major/non-cyber incident outside of the Cyber Security Reporting process	Reg Affairs
4b	Non Major Incident	TDR to manage non-major cyber security incident independently or engage CIM to assist	TDR
5	Contact CIM	TDR contacts CIM that a Major Cyber Security Incident occurred	TDR
6	CIM invoke MIM process	CIM invoke the MIM process and notify FINMA assessment task force	CIM
7	FINMA Assessment required	In the MIM call it will be decided if the FINMA Regulatory Assessment is required	CIM
8	Notify FINMA task force	CIM notifies the FINMA assessment task force if incident meets criteria in section 4	CIM
9	FINMA Task Force assembled	FINMA assessment task force validates the severity criteria and decide if the incident will be reported	FINMA Assessment Task Force
10	Incident report	Decision if the incident will be reported to FINMA based on criteria in section 4 of this document	FINMA Assessment Task Force
11	Send 24 hours notification	Reg Affairs sends the notification to FINMA in the first 24 hours (working days)	Reg Affairs
12	Send 72 hours notification	Reg Affairs sends the report over the FINMA online EHP Portal in the first 72 hours (working days)	Reg Affairs
13	Send root cause analysis	Reg Affairs sends the root cause analysis to FINMA after incident closure	Reg Affairs
14	Create MyIncident	Impacted Business Divisions are responsible to register the incident in MyIncident according to GP-00260	Impacted Business Divisions

PR-XXXXX

8. FINMA assessment Task Force

The CIM team via email distribution list and SMS will notify the FINMA assessment task force once FINMA severity levels are potentially met. The FINMA assessment task force decides if the major cyber security incidents needs to be reported to FINMA.

The FINMA assessment task force consist of the following teams:

- TDR
- CIM
- CISO
- GCIO regional Switzerland lead
- Regulatory Affairs
- Representatives of the affected asset

Support data and information sources

- SVM (if critical external providers are impacted)
- BCM (criticality information accessible and updated periodically)

Names and contact details see following section 9. Teams, Contacts and Roles.

9. Teams, Contacts and Roles

Threat Detection and Response (TDR)

- Identifies cyber security incidents
- Leading the cyber security major incident process
- Maintaining a decision-making capability that will be supported by advisers as necessary

Name	Contacts	Role
Simon Ganiere	Email: simon.ganiere@credit-suisse.com DL: +48 22 359 4110	Cyber Threat Management
Florence Garaud	Email: florence.garaud@credit-suisse.com DL: +41 44 334 30 46	Threat Detection and Response

Central Incident Management Team (CIM)

- Identify the appropriate conference bridge for the incident calls and monitor, facilitate and coordinate the flow of the call. Assist in mobilizing required participants on the call
- Contact the stakeholders necessary for the specific incident
- Ensure an appropriate CS IT Major Incident Manager is assigned and engaged (usually the N4 or N5 of functional area). Assist CS IT Major Incident Manager in gathering information
- Facilitate IT communication flow and accurately log and document the on-going incident based on the agreed decision in terms of communication and information

Name	Contacts	Role
Craig E. Carlos	Email: craig.carlos@credit-suisse.com DL: +1 609 243 1562	Global CIM lead
Massimo Carbona	Email: massimo.carbona@credit-suisse.com	Region CH CIM lead

PR-XXXXX

Name	Contacts	Role
	DL: +41 44 333 22 11	

Chief Information Security Office (CISO)

- Provide advisory on regulatory reporting procedure when required
- Ensure risk advisory and risk management in case of changes in security controls

Name	Contacts	Role
Christopher Girling	Email: Christopher.girling@credit-suisse.com DL: +41 44 333 04 23	CISO Region CH
Valentin Suter	Email: valentin.suter@credit-suisse.com DL : +41 44 332 75 94	Team lead covering region CH

GCIO region Switzerland

- Coordinate involvement of impacted IT / Infrastructure teams

Name	Contacts	Role
Dorothee Schobert-Sargent	Email: dorothee.schobert@credit-suisse.com DL: +41 44 332 42 51	GCIO regional Switzerland lead

Sourcing Vendor Management (SVM)

- Provide information about involved and impacted 3rd Parties in regards to their criticality and regulatory scope
- Inform the task force of contractual agreements

Name	Contacts	Role
Marcus Barnes	Email: marcus.barnes@credit-suisse.com DL: +41 44 332 58 41	Strategy, Sourcing and Execution

Supplier Risk & Control (SRC)

- Provide information about involved and impacted 3rd Parties in regards to their criticality and regulatory scope

Name	Contacts	Role
Friederike Struckmeier	Email: friederike.struckmeier@credit-suisse.com DL: +41 44 3325714	SRC Vendor Risk Management Lead

PR-XXXXX

Business Continuity Management (BCM)

- Provide information about criticality of impacted assets

Name	Contacts	Role
Christoph Schweizer	Email: christoph.schweizer@credit-suisse.com DL: +41 44 333 16 54	BCM Switzerland
Michael Spittler	Email: michael.spittler@credit-suisse.com DL: +41 44 332 99 95	BCM Readiness

Litigation Team

- Analysis the incident and decides if it will be reported to law enforcement

Name	Contacts	Role
Daniel Kläy	Email: daniel.klaey.2@credit-suisse.com DL: +41 44 334 40 46	SUB & IWM Litigation

FINMA Key Contacts

- Recipients of the initial criticality assessment (24h report)
- FINMA contacts for Credit Suisse and Cyber Security topics

Name	Contacts	Role
Simon Brönnimann	Will only be contacted by Reg Affairs	Key Account Manager for CS
Sasa Djokic	Will only be contacted by Reg Affairs	Financial Analyst SME
Sebastian Kunz	Will only be contacted by Reg Affairs	Cyber Security SME

PR-XXXXX

10. Legal Entities

The Credit Suisse owned Legal Entities are aligned as they follow the guidelines from Credit Suisse or are in scope by FINMA. In case the Legal Entity is managing their own IT infrastructure, incident management has to be ensured by the Legal Entity and only FINMA relevant information to be submitted to CS Regulatory Affairs team for submission to FINMA.

To ensure alignment of reported incidents, CISO and Regulatory Affairs have to be involved once FINMA reporting is considered.

Entities managing their own IT infrastructure	Entities with CS managed IT infrastructure
<p>Legal Entities:</p> <ul style="list-style-type: none"> Swisscard BANKnow FIDES Treasury Aventicum 	<p>Legal Entities:</p> <ul style="list-style-type: none"> NAB CS Trust
<p>Duties of the Legal Entity contact:</p> <ul style="list-style-type: none"> Represent the Legal Entity during FINMA reporting process Maintaining a decision-making capability for their Legal Entity that will be supported by advisers as necessary Ensure respective CS teams are involved in timely manner and appropriate communication in their Legal Entity is ensured Provide required information for FINMA reporting 	<p>Duties of the Legal Entity contact:</p> <ul style="list-style-type: none"> Represent the Legal Entity during FINMA reporting process Maintaining a decision-making capability for their Legal Entity that will be supported by advisers as necessary Ensure communication in their Legal Entity is ensured

Swisscard

- Communication to FINMA is done by CS Reg Affairs team
- Maintain own IT infrastructure and therefore inform CS CISO and CS Reg Affairs team in case of a potential major cyber security incident reportable to FINMA
- Point of contact to CS Reg Affairs: Aviva Cohen and Marius Pinggera

Name	Contacts	Role
Daria Meyer	Email: daria.meyer@swisscard.ch DL: +41 44 659 36 86	Head IT Security
Aviva Cohen	Email: Aviva.Cohen@swisscard.ch DL: +41 44 659 34 03	Head of Compliance
Marius Pinggera	Email: Marius.Pinggera@swisscard.ch DL: +41 44 659 33 03	Deputy of Head of Compliance

PR-XXXXX

Neue Aargauer Bank (NAB)

Name	Contacts	Role
Georg Koromzay	Email: georg.koromzay@nab.ch DL: +41 62 838 83 63	LISO

BANKnow

Name	Contacts	Role
Dirk Jonscher	Email: dirk.jonscher@bank-now.ch DL: +41 58 900 55 21	Head of IT Architecture and Security

Aventicum

Name	Contacts	Role
Giovanni Tinella	Email: Giovanni.Tinella@aventicumcapital.com DL: +41 22 518 18 56	LISO

FIDES Treasury AG

Name	Contacts	Role
Samuel Mühlebach	Email: Samuel.Muehlebach@fides.ch DL: +41 44 298 65 14	Security Officer

CS Trust

Name	Contacts	Role
Christian Suter	Email: Christian.suter@credit-suisse.com DL: +41 44 332 59 24	

PR-XXXXX

11. Maintenance of the document

This procedure document will be annually reviewed and where required, revised by CISO.

Whilst this procedure is not a firm policy, the same review cycle for IT policies and standards (as detailed in P-00442, section 4.1) can be followed for guidance or if/when there are significant changes to applications or services supporting this procedure.

PR-XXXXX

Appendix 1: 24h report via email to the FINMA Key Account Managers

We would like to inform FINMA of the occurrence of the potential major cyber security incident outlined below,

Major Cyber Security Incident Report	
Information required	CS input
Name of institution	<i>Credit Suisse Group or entities</i>
Contact person including contact details (telephone and email address)	<i>Reg Affairs is the contact</i>
Date / time of report to FINMA	<i>Reg Affairs</i>
Date / time when attack was discovered	<i>TDR limited management notification email</i>
Date / time of attack (if already known)	<i>TDR limited management notification email</i>
Description of cyber attack and current status	<i>TDR limited management notification email</i>
Initial assessment of severity of the cyber attack	<i>TDR limited management notification email</i>

PR-XXXXX

Appendix 2: 72h report via EHP online system from FINMA

Major Cyber Security Incident Report	
Information required	CS input
Name of institution	<i>Credit Suisse Group or entities</i>
Contact person including contact details (telephone and email address)	<i>Reg Affairs is the contact</i>
Date / time of report to FINMA	<i>Reg Affairs</i>
Date / time when attack was discovered	<i>TDR limited management notification email</i>
Date / time of attack (if already known)	<i>TDR limited management notification email</i>
Description of cyber attack and current status	<i>TDR limited management notification email</i>
Initial assessment of severity of the cyber attack	<i>TDR limited management notification email</i>
Severity trend (<i>selection: decreasing, stable, increasing</i>)	<i>TDR limited management notification email</i>
Affected entities (affected organizational unit(s) within the institution or service provider)	<i>TDR limited management notification email</i>
Affected protective goals (<i>multiple selection: confidentiality, integrity, availability</i>)	<i>TDR limited management notification email</i>
Affected critical functions, business processes or assets (affected information, technology infrastructure, facilities or personnel)	<i>TDR limited management notification email in Business Impact field (input from CIM / MIM Impact Assessment)</i>
Affected number of customers (current status)	<i>TDR limited management notification email (starting point CIM/MIM impact assessment and the affected entities question - needs involvement of the affected business division / third party about customer)</i>
Vectors of attack (<i>multiple selection: email, web-based attack, brute force attack, identity theft, removable media, loss/theft of devices, exploitation of software vulnerability, exploitation of hardware vulnerability, other [define]</i>)	<i>TDR limited management notification email</i>
Type of attack (description) (e.g. DDoS, unauthorized access, malware, misuse of technology infrastructure etc.)	<i>TDR limited management notification email</i>
Administrative, operational and/or technical countermeasures with expected time to effectiveness	<i>TDR limited management notification email</i>
Communication measures (what, to whom, when)	<i>TDR limited management communication and business needs to provide their communication to clients and external customers</i>

PR-XXXXX

Appendix 3: Root Cause Analysis
Incident Closure Report – TDR

PR-XXXXX

Appendix 4: Abbreviations

Abbreviations	Full Name
BCIRP	BCM Cyber Incident Response Framework
BCM	Business Continuity Management
BU	Business Unit
CATI	Continuous Architecture and Technology Improvement
CIM	Central Incident Management
CISO	Chief Information Security Office
CS	Credit Suisse
TDR	Threat Detection and Response
EHP	DE: Erhebungs- und Gesuchsplattform EN: survey and application platform
EUS	End User Support
FINMA	DE: Eidgenössische Finanzmarktaufsicht EN: Swiss Financial Market Supervision Authority
FINMAG	Finanzmarktaufsichtsgesetz
FINMASA	Financial Market Supervision Act
GCIO	Group Chief Information Office
ICTO	Information and Communication Technology Object
IT	Information Technology
MIM	Major Incident Process
PPA	Product, Processes and Activities
RO	Relationship Owner
RTO	Recovery Time Objective
SMS	Short Message Service
SVM	Sourcing Vendor Management