Regulation on Incident Classification

Supplementary regulation to the bLink Participation Contract

Table of Contents

1. Content

This Regulation shall govern the classification, reporting as well as the reporting process of security-related and operational breakdowns by the participants.

2. Background

SIX BBS Ltd ("SIX") shall render the bLink service. Due to the data exchanged, service providers and service users participating in the bLink Platform shall be subject to specific security requirements. Compliance with safety requirements is an essential part of the services rendered to the end customer.

SIX shall render the bLink service towards various participants. In the case of such a high number of financial institutions, clear regulations on the classification of breakdowns and related communication shall be indispensable.

3. Types of Breakdowns

SIX shall distinguish between two types of breakdowns: security-related and operational breakdowns.

Security-related breakdowns shall include any and all breakdowns of the bLink ecosystem, i.e. service providers, platform operators and/or service users, which constitute a data security violation. Such breakdowns shall be treated in accordance with the SIX Security Event and Information Management and use existing information to identify security-related incidents or forensic analysis.

Operational breakdowns shall include any and all breakdowns pertaining to the operation, functionality and availability of the bLink ecosystem, i.e. service providers, platform operators and/or service users. Such breakdowns shall be treated in accordance with the SIX IT Service Management and use existing information describing the functioning of the applications and infrastructure, the deviations from regular functioning as well as other information respectively, to identify the root cause of the breakdown.

4. Breakdown Categories

4.1 Security-Related Breakdowns (SIEM)

Security-related breakdowns shall be classified in accordance with Table 1. The handling of breakdowns shall be categorized as follows:

- Breakdowns classified as critical and serious shall be treated as major incident.
- Breakdowns classified as severe shall be treated as level 2 breakdown under Annex 3 to the Participation Contract.
- Breakdowns classified as minor shall be treated as level 1 breakdown under Annex 3 to the Participation Contract.
- Breakdowns classified as negligible shall not be subject to the Service Level Agreement and shall serve as a measure for internal process control.

4.2 Anomalies in Access Behavior

In accordance with sec. 16 let. a of the Participation Contract, SIX shall examine the anomalies in access behavior. The following provisions shall apply:

1. Detection: SIX shall continuously examine the requests of the service users (24/7) for access irregularities. In particular, it shall check whether a request has been sent by a participant to SIX by means of a combination of identifying characteristics ("Identifying characteristics"), which the participant had earlier reported to SIX (e.g. IP address, and/or certificate) or whether SIX has independently registered a request (e.g. specific behavioral characteristics). Should it not be the case, an irregularity shall be stated. In the course of examination of the participant's request for irregularities, SIX shall exercise customary care.
2. Alerting/incident opening in the Security Operation Center ("SOC") of SIX: Should SIX identify an irregularity as to the request of a participant, the event shall be recorded immediately and a more detailed examination of such irregularity shall be initiated in SOC (24/7) in accordance with the following Section 3.
3. Reaction: SIX shall immediately take appropriate measures to react to the irregularities as soon as possible in order to prevent any unauthorized access to data or otherwise jeopardize the security of the platform or the data exchange processed via it. SIX shall in particular:

   Case a: Immediately prevent a user connection of the participant and block the participant's certificate, respectively the user's certificate, if the identifying characteristics are used for requests from various unknown IP addresses and clarify with the participant within 15 minutes if they use the unknown IP addresses. As soon as the participant confirms that the IP addresses used are valid, the certificate blocking shall be reversed and the IP addresses shall be recorded as part of the identifying characteristics.

   Case b: Clarify with the participant within 15 minutes if they are using an unknown IP address if the identifying characteristics of the participant are being used for a request from such an unknown IP address. If the participant cannot be reached within these 15 minutes or if the participant confirms that they are not using the IP address used, SIX shall immediately preventively block the certificate of the participant or the affected user (certificate). SIX shall further try to contact the participant. As soon as the participant confirms that the IP addresses used are valid, the certificate blocking shall be reversed and the IP addresses shall be recorded as part of the identifying characteristics.

SIX shall no longer process the inquiries with a blocked certificate or inquiries with a blocked IP address. The service user may apply for an IP address to be unblocked or for its blocking to be canceled, should they later prove that they are still using the IP address.

Should a certificate of a service user be blocked, the service providers concerned shall be informed thereof in accordance with Annex 3 to the Participation Contract.

Information Security Incident Severity Matrix

	Level 5 (Negligible)	Level 4 (Minor)	Level 3 (Serious)	Level 2 (Severe)	Level 1 (Critical)
Brand protection (lead by CMC-EC)	Registration of domain name(s) that contains any of the SIX brands without approval (no active use).	Emails impersonating any of the SIX brands to steal credentials (no URL). Unauthorised creation or usage of social media account containing SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including a webpage). Active use of a domain (web, email, etc.) to impersonate any of the SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including good quality webpage impersonating SIX). A non-critical SIX website gets compromised and/or defaced.	SIX corporate or customer-service websites get defaced and/or escalated incident with media exposure.
Data leakage	SIX internal information disclosed externally.	SIX internal information is publicly disclosed or employee information disclosed (<10). SIX customer information disclosed (<10).	SIX confidential information is or SIX customer simple PII information disclosed (1+). SIX employee internal information disclosed (10+). SIX confidential customer information is disclosed (<10).	SIX secret information or customer PII extended information is disclosed (1+). SIX employee confidential or secret information is disclosed (1+). The information is not made public. 100+ records of lower classification is disclosed publicly.	SIX secret (internal and/or customer) or sensitive PII information is disclosed and publicly available (1+). Escalated incident with media exposure.
Denial of service* (lead by CIT-*)	(d)DoS attack with limited impact on SIX operations or reputation. No customer impact.	(d)DoS attack with noticeable impact on SIX operations or reputation. No customer impact.	(d)DoS attack with significant impact on SIX operations or reputation and/or noticeable customer impact.	(d)DoS attack with large impact on SIX operations or reputation and/or significant customer impact.	(d)DoS attack with major impact on SIX operations or reputation and/or large service interruption for a large number of customers.
Malicious code	Malicious code on a single corporate asset. Malicious code in user-managed context.	Same malicious code in user mode on multiple corporate assets (<5).	Same malicious code on multiple corporate assets in user space (<10). Malicious code on single corporate asset with possible escalated privileges.	Same malicious code on multiple corporate assets (10+). Malicious code on multiple corporate assets with confirmed escalated privileges (1+). Malicious code on a high value or crown jewel corporate asset (1).	Malicious code on multiple high value or crown jewel corporate assets (1+), e.g. Active Directory. Escalated incident with media exposure.
Security policy violation	User without administrative privileges violating a security policy not resulting in an incident.	User with local administrator privileges violating a security policy not resulting in an incident. User without admin privileges violating a security policy repeatedly (more than 2 times) or resulting in an incident.	User with local administrative privileges violating the security policy multiple times. User with global administrative privileges violating the security policy not resulting in an incident.	User with global administrative privileges violating the security policy multiple times. User with local admin privileges violating the security policy resulting in an incident.	User with global administrative privileges violating the security policy resulting in an incident or compromise of the account.
Social engineering	Employee being targeted by a generic phishing campaign. Non-harmful message (with or without links or attachments).	Multiple employees being targeted by a generic phishing campaign. Employee that responded to a phishing attack. Phishing attack targeting the banking sector.	Multiple employees that responded to phishing attack. High value employee being targeted by phishing campaign. Employee(s) being targeted by a phishing campaign for high value information. Phishing attack targeting SIX specifically.	Employee(s) that responded to phishing attack with financial impact/loss or data disclosure. Multiple high value employees being targeted by phishing campaign.	Escalated incident with financial impact, loss or data disclosure.
System vulnerability	Attackers can collect information about the host via open ports, services, software versions, OS, etc. leading to disclosure of other vulnerabilities. CVSS V3 0.1 - 3.9 score.	Attackers can collect sensitive information about the host leading to disclosure of other known vulnerabilities. CVSS V3 4.0 - 6.9 score.	Publicly available & known vulnerabilty with attackers potentially having access to security settings, disclosure of file contents, directory browsing, read access to files etc. CVSS V3 7.0 - 8.9 score.	Publicly avialable & known vulnerability where attackers can gain control of the host, collect confidential information or execute commands remotely or cause a DoS scenario. Vulnerability specific to the banking sector. CVSS V3 9.0 - 10.0 score.	Attackers can easily gain control of a host (or multiple), which can lead to the compromise of the entire network. Severe vulnerability actively exploited in the wild and/or resulting in a DoS scenario for a cricital service. Escalated incident with media exposure.
Unauthorised access	Customer credentials being used on SIX service by an unauthorised party. Network scanning activity by an unknown party on resources exposed to the internet.	Multiple customer credentials being used on SIX service by an unauthorised party. Employee credentials being used by an unauthorised party.	Multiple employees credentials being used by an unauthorised party.	High value employee credentials being used by an unauthorised party. Social media account being used by an unauthorised party.	Multiple high value employee credentials being used by an unauthorised party. Escalated incident with media exposure.

Table 1: Levels of security-related breakdowns

4.3 Operational Breakdowns (Incidents)

In case of operational breakdowns, the impact of the breakdown and the urgency of breakdown removal shall be assessed. The impact shall be evaluated on a 4-step scale:

1– large-scale impact

2 – significant/strong impact

3 – moderate/limited impact

4 – small/located impact

The urgency shall also be evaluated on a 4-step scale (1 – serious, 2 – middle, 3 – high, 4 – critical).

The combination of both values shall determine the priority of breakdown removal in accordance with Table 2.

The handling of breakdowns shall be categorized as follows:

- Breakdowns having the priority critical or high shall be treated as major incident under Annex 3 to the Participation Contract.
- Breakdowns having the priority severe shall be treated as level 2 breakdown under Annex 3 to the Participation Contract.
- Breakdowns having the priority low shall be treated as level 1 breakdown under Annex 3 to the Participation Contract.

Impact	Urgency	Priority
1 - Extensive/Widespread	1 - Critical	Critical
2 - Significant/Large	1 - Critical	Critical
1 - Extensive/Widespread	2 - High	Critical
3 - Moderate/Limited	1 - Critical	High
2 - Significant/Large	2 - High	High
4 – Minor/Localized	1 - Critical	High
1 - Extensive/Widespread	3 - Medium	High
3 - Moderate/Limited	2 - High	High
2 - Significant/Large	3 - Medium	Medium
4 – Minor/Localized	2 - High	Medium
3 - Moderate/Limited	3 - Medium	Medium
4 – Minor/Localized	3 - Medium	Medium
1 - Extensive/Widespread	4 - Low	Low
2 - Significant/Large	4 - Low	Low
3 - Moderate/Limited	4 - Low	Low
4 – Minor/Localized	4 - Low	Low

Table 2: Priority of operational breakdowns

5. Breakdown Reporting Process

Breakdown reporting process relevant for the participants (part of incident management) shall be presented in Figure 1.

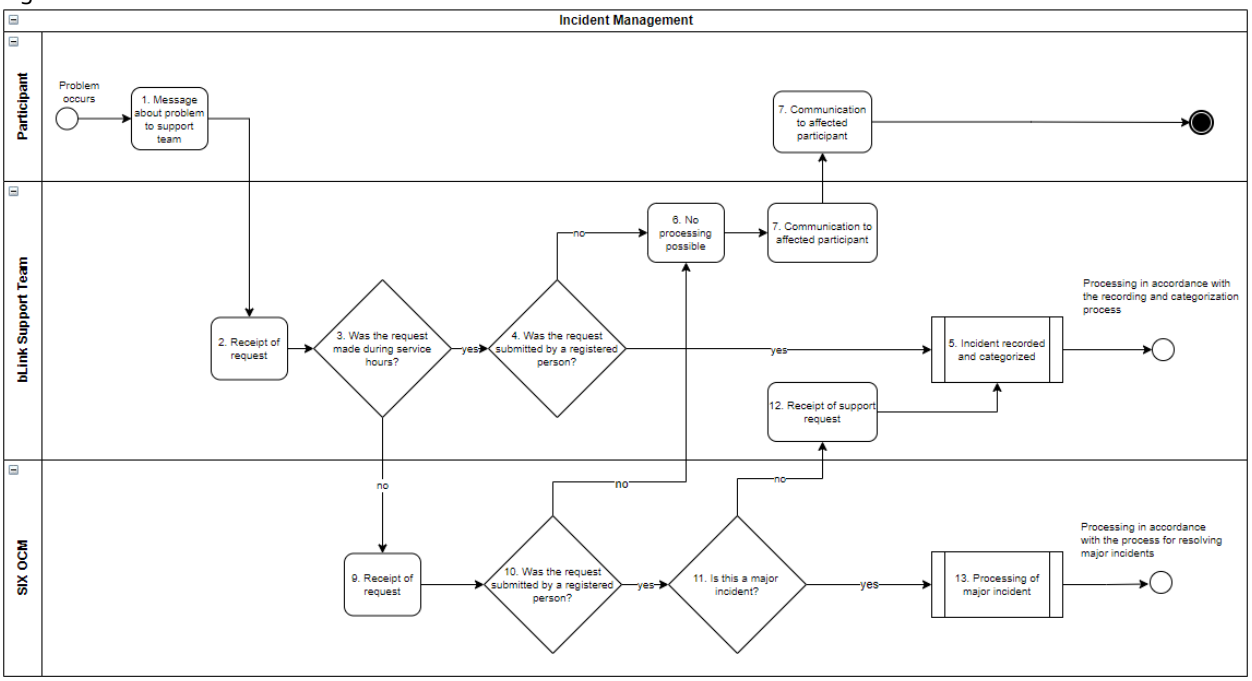

Figure 1: Breakdown reporting process

1. The participant shall report their problem regardless of its scope and regardless of the support hours of the support team of SIX defined in the Service Level Agreement.
   Note: The process shall also be triggered in the event of breakdowns detected by the internal monitoring system of SIX.
2. The report of the participant shall be forwarded to the bLink support team via phone or e-mail.
3. First of all, it shall be clarified whether the inquiry was received during the support hours specified in Annex 3 to the Participation Contract. Should the inquiry be submitted outside the support hours, steps 4 to 8 may be skipped.
4. Should the inquiry be submitted during the support hours, it shall be subsequently clarified whether it was submitted by a person authorized for support purposes. A detailed regulation on the authorization of persons for support purposes shall be governed under chapter 4 of Annex 3 to the Participation Contract. Should it not be the case, step 6 shall apply directly.
5. Should the inquiry be submitted by an authorized person, the inquiry shall be recorded and categorized. Subsequently, the inquiry shall be processed in accordance with the internal process of SIX to remove breakdowns.
6. Should the inquiry be submitted by a person not authorized for support purposes, it shall not be processed.
7. In such case, the support team shall inform the participant that the inquiry cannot be processed due to lacking authorization.
8. The participant shall receive a notification that their inquiry could not be processed due to lacking authorization.
9. Should the inquiry of the participant be submitted outside the support hours, it shall automatically be forwarded to the OCM or in case of a security-related breakdown to the SOC (part of the OCM).

10. Moreover, in case the inquiry was submitted outside the support hours, it shall be clarified whether it was submitted by a person authorized for support purposes. Should it not be the case, the OCM/SOC shall take steps 6–8 and inform the participant concerned.
11. Should the inquiry be submitted by a person authorized for support purposes, the OCM/SOC shall decide whether it pertains to a major incident or to a support inquiry having no time-critical character.
12. Should the inquiry pertain to a major incident, it shall be treated in accordance with the process to remove breakdowns.
13. Should the inquiry to the OCM/SOC not pertain to a major incident and be submitted outside the support hours, it shall be returned to the support team that shall process it in accordance with the documented process under Annex 1 on the following working day.

6. Confidentiality

Any breakdown reporting, descriptions and status shall be deemed confidential and shall not be disclosed to any third parties. The participants shall not be considered third parties. Forwarding information among the participants shall take place within the “need-to-know principle” only.

7. Reviewing of This Regulation

SIX shall review and evaluate the adequacy and effectiveness of the provisions specified in this Regulation on a periodical basis.

Any changes to this Regulation shall be subject to the provisions of the Participation Contract.

8. Escalation Mechanism

The escalation mechanism under Annex 3 to the Participation Contract shall apply.

9. Effective Date

This Regulation shall come into force as of 1 January 2022.