Code of Practice for the Digital Trust Label

Version 1 - October 2021

Swiss Digital Initiative
c/o Campus Biotech
Chemin des Mines 9
1202 Geneva
Switzerland

© 2021 Swiss Digital Initiative.
Digital Trust Label.
All rights reserved.

SWISS DIGITAL INITIATIVE

PART I: CERTIFICATION PROCESS AND RULES

1. AUDIT PROCESS

1.1 Scoping meeting

The goal of the scoping meeting is to gather all the information needed to prepare the offer. The standard agenda includes the following topics:

AGENDA:

0 SGS: Presentation of SGS
1 Client: Presentation of the client's company
2 SGS: Brief overview of DTL requirements and the documents to be delivered
3 Client: Presentation of the product/online service to be labelled
- Internal processes – outsourced processes
- Relevant external audits (by financial advisor, certification body etc.)

4 Decision on final scope (level of complexity)
5 Audit duration / Audit costs
6 SGS: Audit process
7 SGS: Next steps

1.2 Offer issuance and contract signing

The client completes the DTL-questionnaire and gets then the offer. If requested, a Non-Disclosure Agreement NDA is signed first.

1.3 Audit steps

STAGE 1

The client completes the audit checklists with the relevant company-specific documents: mainly templates, but also records as far as they are allowed to be handed out;

The client gives access to the documents; the data transfer has to be mutually agreed at the scoping meeting (We-Transfer, E-Mail etc.); IT security is fully ensured.

The auditor checks the completion of the documents and their content in a document review and completes the audit report with the minor or major findings/nonconformities. Major nonconformities shall be removed before Stage 2 Audit can be started.

STAGE 2

Stage 2 Audit takes place as a TEAMS meeting and includes the following topics:

- Opening meeting
- Formal closing of findings out of Stage 1 Audit
- Verification of the records according to the audit checklist
- Evaluation among the auditors
- Final meeting: Disclosure of the audit result and agreement on the next steps.

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

1.4 Label Issue

After having closed all the nonconformities, the final audit report will be forwarded to SDI for technical review and granting the label. The label is valid for three years.

1.5 Following Audits

- Surveillance audit takes place after one year with the objective to evaluate the maintenance of the relevant procedures and associated documents (templates and records);
- Renewal Audit ≈ Stage 2 Audit

1.6 Early Renewal

Early renewal is due in case of a new release of the product (major changes of the features). Stage 1 audit will be required depending on the level of changes. This decision is taken in a shortened scoping meeting and the LA justifies it in a documented manner

1.7 Transition Audit

A transition audit is due in case of a standard version update. Transition period/transition audit type will be defined by SDI case-by-case depending on the urgency of the implementation of the new rules and the level of changes. There are the following options:

- Within x months from the publication date -> separate transition audit: new certificate valid until the current expiry date;
- At the next following audit (surveillance or renewal audit) -> in case of surveillance audit: new certificate valid until the current expiry date;
- At the next regular renewal audit: new certificate with new expiry date;
- Start the audit process from new: Stage 1+2 audit (rather unlikely).

2. DUE DATES

The audits shall be completed within the following timeframe:

- Stage 2 Audit: Not later than three months after Stage 1 Audit;
- Surveillance Audit: +/- 2 months from the Due Date (= date of the last Stage 2 Audit date);
- Renewal Audit: ≤3 months before the Due Date; (= date of the last Stage 2 Audit date);
- Closing of nonconformities: 90 days after the last audit day;

Note: In case of open nonconformities at the expiry date, the new certificate will have a shortened validity:

Example

- Due date (last day of Initial Audit / Stage 2): 15 July 2021
- Certificate date: 30 July 2021 (after reporting, technical review, and certification decision)
- Certificate validity: 30 July 2021 to **29 July 2024**
- Start of Renewal Audit: 15 May 2024
- Closing of nonconformities: 15 August 2024
- Certificate validity: 15 August 2024 to **29 July 2027**

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

3. NONCONFORMITIES

4.1 Types of Nonconformities

- MAJOR NC: Failure which impacts a critical risk concerning IT security, data protection and/or fair user management (missing system elements, lack of implementation etc.);
- MINOR NC: Failure which impacts a limited risk concerning IT security, data protection and/or fair user management;

4.2 Closing of Nonconformities

- MAJOR NC: Action plan to be issued within 30 days; Follow-Up-Audit to be performed within 90 days;
- MINOR NC: Action plan to be issued within 90 days; the implementation of the actions will be checked during the next following regular audit.

Overdues cause any suspension of the label which lasts another 30 days at maximum. Afterwards the label will be withdrawn.

PART II: AUDIT DURATION

The certificate is valid for 3 years, provided the annual surveillance audits are passed. The audit duration (number of audit days) is calculated based on the complexity of the product.

We differentiate the following levels:

Level	Definition
Level 1	Regular system or device, for example this can be - A server/client infrastructure which consists of one backend service (e.g. Application and Database) and one to two frontend services (e.g. Client Application, Web Application, mobile App, API) - A connected device (e.g. IoT) with one companion application (mobile, PC application) and one Backend Service The service also should rely on not more than one additional external third-party service, e.g. for payments or authentication.
Level 2	Larger systems, in which more backend and/or frontend services are involved, or which consist of more than one device or multiple companion apps or backends: - A server/client infrastructure with either two backend services or 3-4 frontend services - Either two coupled connected devices or 2-3 companion apps or 2 backend services The service can rely on up to three additional external third-party service, e.g. for payments or authentication.
Level 3	Complex systems, in which more backend and/or frontend services are involved, or which consist of more devices, companion apps or backends: - A server/client infrastructure with two backend services and 3-4 frontend services - A server/client infrastructure with three backend services - A server/client infrastructure with 5-6 frontend services - Two coupled connected devices and/or 2-3 companion apps and/or 2 backend services (2 out of 3) The service can rely on up to five additional external third-party service, e.g. for payments or authentication.
Level 4	Very complex systems, which go beyond the limitations of Complexity Level 3

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

INITIAL AUDIT

Level of complexity	CHF	Audit duration including preparation & report	
		Stage 1	Stage 2
1	10'000	2 days	2 days
2	14'000	3 days	3 days
3	18'000	4 days	4 days
4	22'000	5 days	5 days
>4	to be calculated case-by-case; the offer shall be approved by SDI.		

SURVEILLANCE AUDIT

Level of complexity	CHF	Surveillance Audit
1	3'000	1 days
2	4'000	1.5 days
3	5'000	2 days
4	6'000	2.5 days
>4	to be calculated case-by-case; the offer shall be approved by SDI.	

RENEWAL AUDIT

Level of complexity	CHF	Renewal Audit
1	6'000	2 days
2	8'000	3 days
3	10'000	4 days
4	12'000	5 days
>4	to be calculated case-by-case; the offer shall be approved by SDI.	

The following aspects cause some reduction/increase of the standard audit duration. The % shall be defined case-by-case at the scoping meeting.

Increase of audit duration (10-30%):

- The hosting infrastructure (often provided by a third party and not the company itself) is not certified against ISO 27001 by an acknowledged Certification Body;
- There are multiple (independent) development teams involved.

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

Reduction of audit duration (10-30%):

- The company is certified against ISO 27001 and/or ISO 22301 by an acknowledged Certification Body;
- There are outsourced processes/parts (e.g. data storage), provided an ISO 27001 certificate or supplier audit is available;
- Some processes are audited by another body, provided the audit has been performed by an acknowledged company (e.g. financial advisor like PwC, KPMG etc.) and against an official standard;

PART III: SDI LABEL FEES

SDI LABEL FEE FOR THE DIGITAL TRUST LABEL

Level of complexity	CHF – total fee	CHF – to be paid upfront	CHF – to be paid after the successful audit
1	6'000	3'000	3'000
2	7'900	3'950	3'950
3	10'000	5'000	5'000
4	11'250	5'625	5'625
>4	upon request		

The SDI label fee is a fixed fee and depends on the complexity of the digital service. The fee is valid for the label validity duration.

The fee will be invoiced in two equal parts:

- Label subscription fee: To be paid upfront, non-refundable in case of an unsuccessful audit
- Label labelling fee: To be paid upon the successful audit, non-refundable

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

Disclaimer: This document has been prepared only for purposes of the use of the recipient and only serves for the scope and the terms agreed. This document may not be reproduced or circulated without the Swiss Digital Initiative's prior written consent. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else. © 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.

© 2021 Swiss Digital Initiative. Digital Trust Label. All rights reserved.