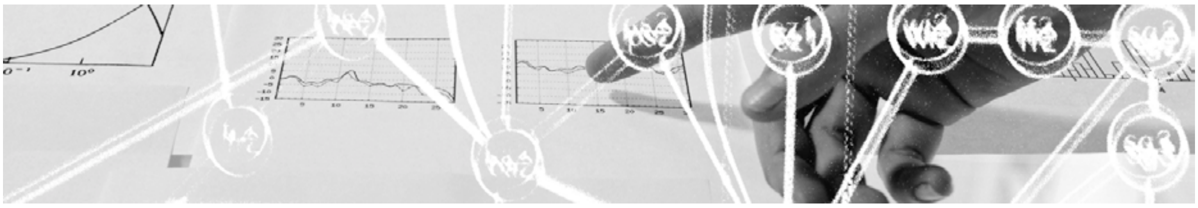
SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

AAI Maturity Scan

Final report, 2012



Thomas Lenggenhager, SWITCH

Rolf Grau, Daniela Roesti, CSI Consulting AG

Version: V1.00, 17 October 2012

URL: http://switch.ch/aai/docs/AAI_Maturity_Scan_Report_2012.pdf

1 Summary

SWITCH devised the AAI Maturity Scan to enable Home Organizations of the SWITCHaai federation to assess their AAI maturity level and to gain at the same time a better understanding about trust level of SWITCHaai enabled accounts at volunteer institutions.

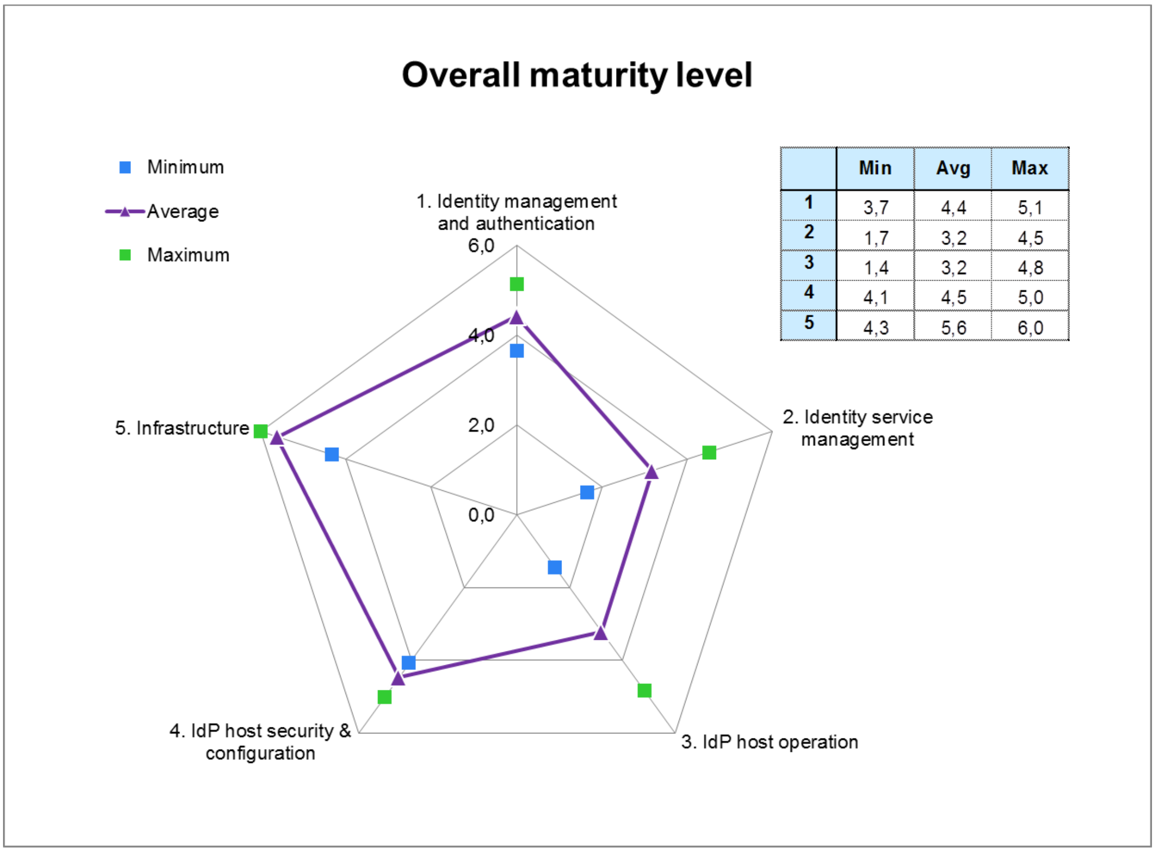
The investigation was done in two phases:

- Pilot Phase (phase 1)
- Interview Phase (phase 2)

In the pilot phase a questionnaire was developed and tested by interviewing four Home Organizations. The results were an optimized questionnaire [2] and its evaluation tool together with the evaluated maturity level for each organization [4].

This report describes overall results and findings of phases 1 and 2 of this AAI Maturity Scan in which a total number of nine Home Organizations answered the questionnaire (see Table 1 on the next page).

Figure 1 below summarizes the results of all nine participating Home Organizations:



	Min	Avg	Max
1	3,7	4,4	5,1
2	1,7	3,2	4,5
3	1,4	3,2	4,8
4	4,1	4,5	5,0
5	4,3	5,6	6,0

Figure 1: Evaluated maturity level for phases 1 and 2, 2011 - 2012

The strengths of the participating organizations are in the areas of ‘Identity management and authentication’, ‘IdP host security and configuration’ and ‘Infrastructure’. Room for improvement lies especially in the areas of ‘Identity service management’ and ‘IdP host operation’.

Phase 1	Phase 2
Fachhochschule Nordwestschweiz	Berner Fachhochschule
Universität Basel	Ecole Polytechnique Fédérale de Lausanne
Université de Fribourg	Hochschule Luzern
Université de Lausanne	Université de Genève
	Universität Zürich

Table 1: Participating Home Organizations

Out of 47 Home Organizations that run an IdP, roughly 20% participated in this survey. However, looking at the number of AAI enabled user accounts, the participating organizations represent 46% of a total of 350'000 - mainly bigger institutions volunteered.

Each participating Home Organization received a detailed report with their own results, together with recommendations for optimization steps.

For all other Home Organizations this report could well serve, together with the questionnaire, as a starting point to effectively review and optimize their own Identity Management and AAI Identity Provider setup.

Based on the observations and findings during the AAI Maturity Scan, SWITCH will revise and improve the AAI Best Current Practices (BCP) document [1].

2 Objectives of the maturity scan

In Switzerland, AAI is well established and in production use since 2005. 47 Home Organizations are operating an Identity Provider (IdP)[1] in SWITCHaai, so that 98% of all higher education users have an AAI enabled account. The identity management is an essential basis for the operation of an IdP. The Service Providers (SP), which protect the access to their web applications, trust the IdP and identity management of the corresponding Home Organization.

After having reached good coverage, the next goal is to take a closer look at the quality of AAI. First steps into this direction were the Best Current Practices Documents [1] for operating an IdP and SP within the SWITCHaai federation. As a next activity, the AAI Maturity Scan was undertaken, motivated by the experience of a similar study in The Netherlands: In 2009, the Dutch national research and education institution SURFnet performed an identity maturity scan for Dutch universities, which was well received. In the future, optional Identity Assurance Profiles will enable SPs knowing more about the quality of an identity. Identity Assurance Profiles define requirements for an IdP Operator regarding digital identities it manages and for which it issues assertions.

The maturity scan offers three benefits for the administrator of a participating Home Organization:

- Compare the maturity of their identity management with the average, minimum and maximum of other Home Organizations
- Determine where they can improve their identity management
- Determine their maturity level as a mean to provide Service Providers (SP) an indication on the level of trust they can have towards their Home Organization.

[1] The terminology of SWITCHaai understands the IdP as a software unit, which technically performs the authentication and makes the authentication attributes available to the Service Providers as a SAML assertion.

3 Participating Home Organizations

The following Home Organizations participated in the AAI Maturity Scan. From each Home Organization participated the IdP administrator as well as the IdM service manager or another person involved in identity management:

Pilot phase:

- Fachhochschule Nordwestschweiz, 7 September 2011,
- Universität Basel, 26 August 2011,
- Université de Fribourg, 20 September 2011,
- Université de Lausanne, 30 August 2011.

Interview phase:

- Berner Fachhochschule, 18 September 2012,
- Ecole Polytechnique Fédérale de Lausanne, 13 June 2012,
- Hochschule Luzern, 10 July 2012,
- Université de Genève, 03 July 2012,
- Universität Zürich, 12 June 2012.

Only Home Organizations out of the higher education sector have volunteered to participate in this survey. The six universities and the three universities of applied sciences represent 26% of the total number of Home Organizations in this sector. None of the teacher education universities decided to participate as well as none of the institutions of the other sectors: hospitals, libraries and research institutions.

The interviews were conducted by a team, guided by

- Thomas Lenggenhager, SWITCHaai project manager, SWITCH
- Lukas Hämmerle, Software Engineer, SWITCH (for BFH only)

with the support of

- Thomas Siegenthaler, CSI Consulting AG (for phase 1)
- Rolf Grau, CSI Consulting AG (for phase 2)
- Daniela Roesti, CSI Consulting AG

4 Methodology

The AAI Maturity Scan was done in two phases:

- Pilot Phase (phase 1)
- Interview Phase (phase 2)

In the pilot phase (phase 1), a questionnaire was developed and tested by interviewing four Home Organizations. The results were an optimized questionnaire [2] and its evaluation tool, together with the evaluated maturity level for each organization [4].
In the interview phase (phase 2), all interested Home Organizations within the AAI federation could take part in the investigation to evaluate their AAI maturity level.

4.1 Standardized questionnaire and evaluation procedure

In order to guarantee a professional IdP operation within SWITCHaai, SWITCH published the document “Best Current Practices for operating a SWITCHaai Identity Provider” (BCP) [1], which contains requirements and suggestions (reflecting best common practices) for the IdP operators. This BCP document was the basis to elaborate the questionnaire for the structured interview. The questionnaire consists of five main criteria:

1. Identity management and authentication,
2. Identity service management,
3. IdP host operation,
4. IdP host security & configuration,
5. Infrastructure.

Accordingly, the maturity level consists of five values, which allow a more specific comparison between the different participating organizations.
These five main criteria are composed of different sub criteria; and every single criterion was rated with four grades:

6 ‘fulfilled’: all requirements and most suggestions fulfilled[2]
4 ‘partly fulfilled’: requirements/suggestions are partly fulfilled
2 ‘insufficiently fulfilled’: requirements not fulfilled, few suggestions fulfilled
0 ‘not fulfilled’.

The individual weight of each criterion was determined by considering the amount of corresponding requirements and suggestions in the BCP.

4.2 General procedure applied for interviews

Preparation of the interview:

- The Home Organization signed up at SWITCH for the AAI Maturity Scan.
- The Home Organization received the questionnaire ‘Identity Management Maturity Scan for SWITCHaai’ and the meeting date was defined.
- The Home Organization identified its representatives and prepared the interview; however, it was not necessary to prepare written answers prior to the interview.

[2] ‘All suggestions fulfilled’ – in cases where only suggestions (and no requirements) are rated.

During the interview:

- After a general introduction to the subject, a couple of first questions were asked to better understand the local environment.
- The interviewer elaborated on the questions and ensured that they are properly understood so that the answers could be consistently evaluated with respect to the other institutions. The interview lasted at most 3 hours. The Home Organization was typically represented by the two roles 'IdM service manager' and 'IdP administrator'.
- The interview team took written notes, as a SWITCH-internal document to support the evaluation procedure. These were not handed over to the Home Organization.

After the interview:

- The interviewing team evaluated the maturity level through the standardized evaluation procedure described below.
- The results were reported in a dedicated 'AAI-Maturity report' which is delivered to each participating Home Organization (see the Addendum for a sample).

5 Scope of the AAI Maturity Scan

The scope of the identity management maturity scan for AAI is shown below in Figure 2. SWITCHaai is composed of central elements (components and processes), the IdP elements of each Home Organization and all SP elements of AAI Federation Members and Federation Partners. The maturity scan (shaded area) focuses on the IdP elements of the Home Organization and the identity management for all data sources that can be accessed within the Home Organization.

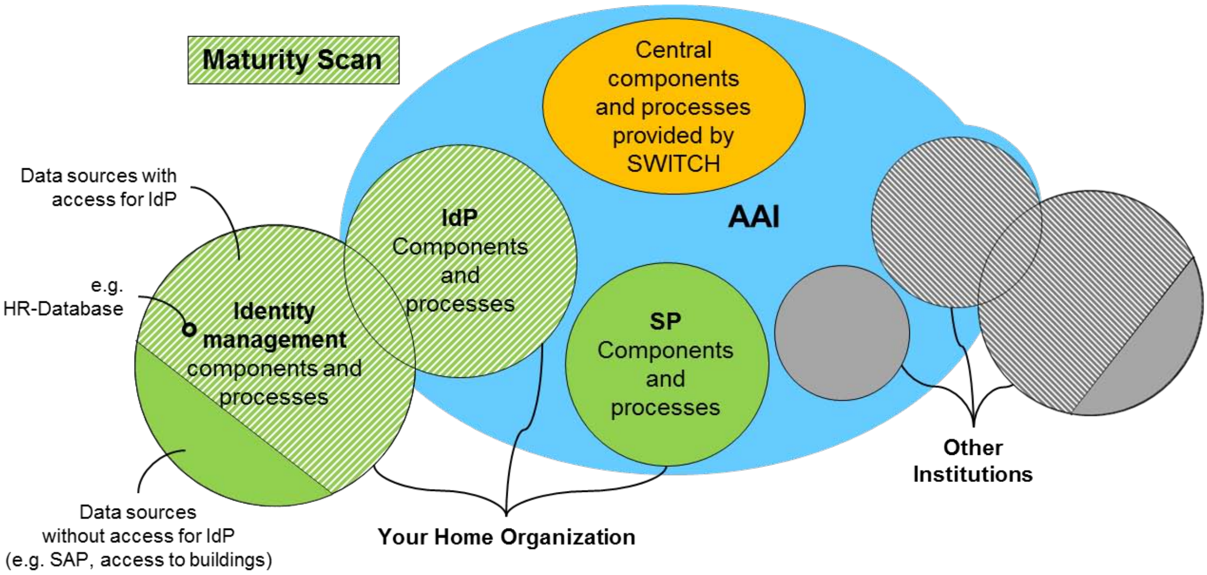
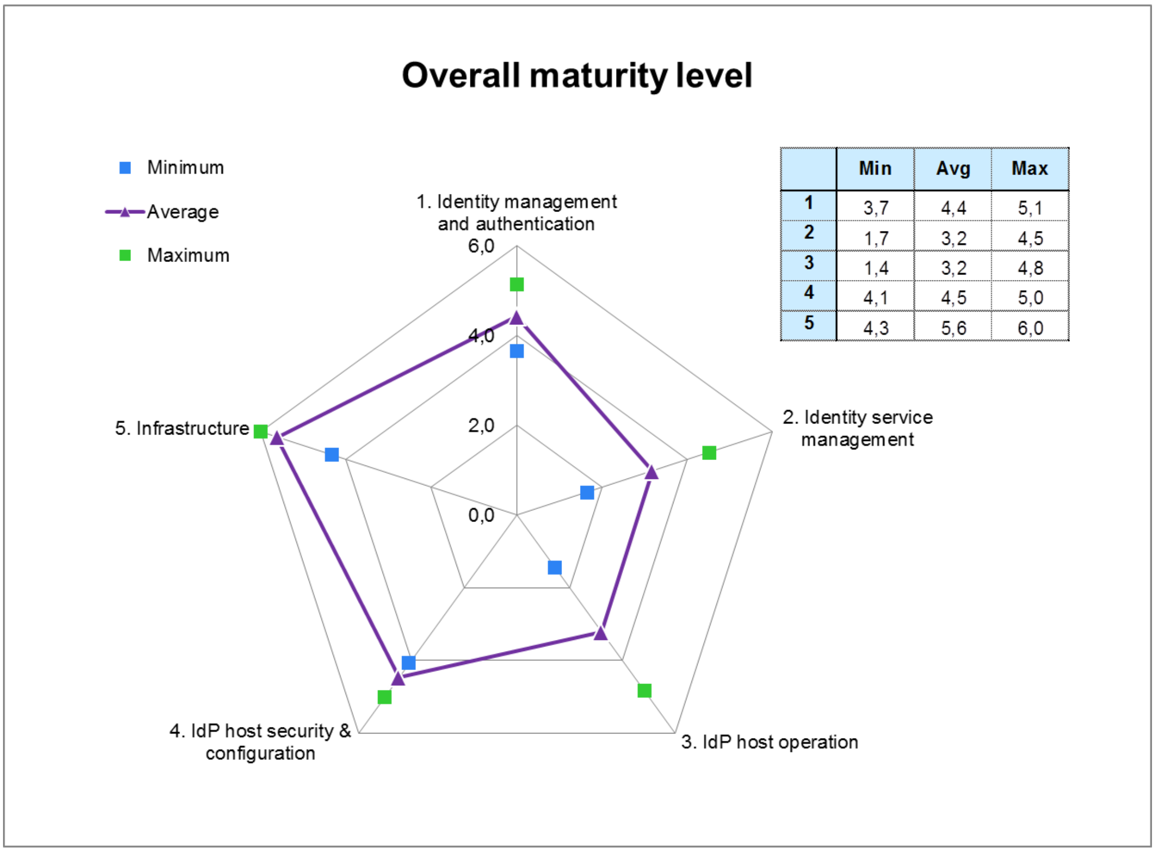

Maturity Scan
Central components and processes provided by SWITCH
AAI
Data sources with access for IdP
e.g. HR-Database
IdP Components and processes
Identity management components and processes
SP Components and processes
Data sources without access for IdP (e.g. SAP, access to buildings)
Your Home Organization
Other Institutions

Figure 2: Scope of maturity scan

6 Evaluated maturity levels (results of phase 1 and 2)

Figure 3 shows for all five main criteria the average maturity level reached in the pilot and interview phase by the nine participating Home Organizations. The minimum and maximum values reached for each main criterion are also shown. A rating value of 4 indicates that the criterion is only ‘partly fulfilled’ and optimizations are necessary.



	Min	Avg	Max
1	3,7	4,4	5,1
2	1,7	3,2	4,5
3	1,4	3,2	4,8
4	4,1	4,5	5,0
5	4,3	5,6	6,0

Figure 3: Evaluated maturity level for phases 1 and 2 (nine participants)

According to Figure 3 the best results were reached for the main criterion ‘Infrastructure’ (criterion 5). The average value is close to ’fulfilled’. Only the server room access control could be optimized in some cases.

The two criteria ‘Identity management and authentication’ (criterion 1) and ‘IdP Host Security & Configuration’ (criterion 4) reached average values of 4.4 and 4.5 respectively (i.e. ‘partly fulfilled’), which means that some optimizations are necessary. Criterion 1’s problem areas are: policy, processes, reporting, review and audits as well as strong authentication. Criterion 4’s problem areas are: strong authentication access to IdP, root password and management accounts, process for revoking keys, version control, and regular review of Resource Registry settings.

The two main criteria ‘Identity Service Management’ (criterion 2) and ‘IdP Host Operation’ (criterion 3) reached only average values of 3.2 (i.e. ‘insufficiently fulfilled’) with a considerable variance in the results. Here, optimizations are urgently needed.
Criterion 2’s problem areas are: disaster recovery procedure, maintenance windows, service level descriptions, review of the IdP Emergency Disabling Procedure (IdP Revocation) and statistical data reporting.
Criterion 3’s problem areas are: monitoring, alerting, access control to log files, test of restore procedure and documentation.

The participating Home Organizations find specific hints in their detailed report (see the Addendum for a sample).

Generally speaking, Home Organizations that underwent a major reorganisation or other change recently seemed to score better – possibly because this is a good opportunity to review and update systems and processes.
There does not seem to be any correlation between size (students and personnel) or budget and AAI Maturity Scan performance.
Primarily the smaller Home Organizations from the higher education sector as well as the ones from the other sectors did not participate.

7 Additional findings

Several Home Organizations do not assign Identity Management Service Manager and System Administrator roles (and deputies) to specific persons, but rather to support teams.

Some Home Organizations say they do not need and define any maintenance window, because they can guarantee 24x7 uptime by providing a combination of hot-standby infrastructure (active-active), virtual servers on hardware clusters, system snapshots as fall-back mechanism or using infrastructure lifecycle management tools like the open source Puppet. As a consequence, they no longer backup server systems and do no disaster-recovery testing either.

Some Home Organizations have decided to explicitly not enforce regular password change for users or administrators; instead they always enforce very strong passwords. Only few organizations are yet planning to deploy stronger authentication methods than username and password. The use cases justifying an additional effort in this field seem still to be scarce.

Some organizations do not allow use of root login and passwords on servers (but they still set an initial root password). Some organizations, using consistently “sudo” for root tasks, have no password defined for the root account at all – by consequence they do not need to change it.

Monitoring on the OS and system level is well established, however, application specific monitoring beyond port connectivity is seldom deployed. Regular reporting based on the data collected for the monitoring is mostly missing.

One Home Organization suggests that the BCP document should also include “How to” examples.

Most respondents have integrated their e-learning platforms into SWITCHaai. However, some organizations go much further by also integrating their HR, student administration or even financial web browser-based platforms. Other applications used through SWITCHaai include group collaboration (e.g. with the SWITCHtoolbox), wikis, document exchange or software download.

Home Organizations could increase the benefit their users get from AAI by considering to integrate further local web applications into SWITCHaai or by promoting the use of AAI enabled applications already offered by other AAI participants.

8 Outlook

SWITCH distributes this report to all Home Organizations of SWITCHaai in order to raise their interest in continually improving quality of and hence confidence in their own AAI.

Home Organizations are also encouraged to get in touch with each other directly, in order to interchange knowledge and experience, and to improve overall as an AAI federation. We encourage Home Organizations still interested in having their AAI Maturity Level reviewed to contact SWITCHaai <aai@switch.ch>.

A major step beyond this AAI Maturity Scan would be a much more formal assurance program, like the one launched by the US InCommon Federation with its two profiles Bronze and Silver [5]. The considerable effort to establish such an assurance framework requires strong use cases that promise to justify the resources required to build the framework and to certify Home Organizations. In the US, these use cases originate from upcoming higher-risk applications from the National Institutes of Health (e.g. for federated grant submission) or the National Student Clearinghouse (for access to private and federal loan reports). These applications require increased trust of the Home Organization's authentication and identity management system.

Up to now, no comparable requirements from SWITCHaai participants are known. Get in touch with SWITCH if you are aware of such potential requirements!

9 Referenced documents

[1] ‘Best current practices for operating a SWITCHaai Identity Provider’
see: http://www.switch.ch/aai/bcp

[2] Questionnaire of the Identity Management Maturity Scan for SWITCHaai
see: http://www.switch.ch/aai/docs/Maturity_Scan_Questionnaire.pdf

[3] AAI-Website
see: http://www.switch.ch/aai

[4] ‘AAI Maturity Scan – Report for pilot phase 2011’
see: http://www.switch.ch/aai/docs/AAI_Maturity_Scan_Report_2011.pdf

[5] InCommon Assurance Program
see: http://www.incommon.org/assurance

Addendum

Structure of the report ‘AAI Maturity Scan’ delivered to the Home Organization

The report delivered to the Home Organization contains its evaluated maturity level with a spider graph like in Figure 3 and specific recommendations to the Home Organization for improvements and has the following structure:

1 Summary
2 Interview
3 Objectives of the AAI maturity scan
4 Applied methodology
5 Scope of the AAI maturity Scan
6 Evaluated maturity scan
7 Recommendations for improvements
7.1 General recommendations
7.2 Specific Recommendations for the Home Organization
8 Referenced Documents
9 Appendix

The Appendix chapter contains a detailed overview of all criteria which have been rated as ‘insufficiently fulfilled’ such that the Home Organization can evaluate their own measures for improvements. The following is a sample what chapter 9 (appendix) of the report looks like. The table below shows as an example what the specific recommendations for criterion 3 ‘IdP host operation’ could look like.

3. IdP host operation

Criterion	Recommendation
3.1.2	Alert if CPU, memory or disk usage exceeds 60, 80 resp. 75%. (S071-73)
3.1.4	Monitor webserver log files. (R076)
3.1.5	Monitor application container log files, IdP log files and data source log files for error or warning entries. (R077 and S078)
3.2.1	Ensure by documentation and verify that only permitted staff have access to the log files regularly. (R083)
3.2.3	Define a process which ensures that user identifying data is anonymized when copies of log files leave the organization. (R088)
3.3.2	Ensure that backups are stored in an offsite and secure location. (S093)
3.3.3	Test the restore procedure at least twice a year on your IdP. (S095)