# CAcert Internal Audit

**Audit Programme 2014 - 2016**

Benedikt Heintel

May 31, 2014

Version 1.2

# Contents

# 1 Introduction

This is CAcert's first internal audit programme under the new internal lead auditor Benedikt Heintel. Scope of the audit is the prove of compliance to CAcert's Policies in the first step and the check against external audit / certification readiness in a second step.

This audit programme follows the international norm ISO 19011:2011 and is carried by CAcert's Committee in motion m20131206.6.

This Audit plan contains all the information about audit planning, audit execution, audit monitoring, and audit improvement. Chapter 2 explains the management of the audit programme and its extends. The following Chapter 3, 4, 5 detail the audit programm within the individual audit plans for each year covered by this audit programme.

# 2 Audit Programme

## 2.1 Objectives

This audit programme is created to prove CAcert's maturity

- to determine the effectiveness of the management system,
- to contribute to the improvement of the management system,
- to fulfill the need for compliance with CA/Browser Forum's baseline requirements,
- to verify conformity with contractual requirements from CCA,
- to obtain and maintain the community's confidence in CAcert, and
- to evaluate the compatibility and alignment of the management system objectives with CAcert's overall organisational objectives.

## 2.2 Roles and responsibilities

Auditors are the main resource in an audit, it is important, that auditors have the required competences to fulfill their duty. Where the knowledge of the auditors is limited, specialist might help out and work with the auditors. The next sections contain the main skills and tasks of these audit participants.

### 2.2.1 Lead auditor

The lead auditor is entitled to create, execute, monitor, review and improve CAcert's internal audit programme. She is further authorised to nominate auditors and delegate duties towards them.

Skills and competences of a lead auditor are:

- knowledge of audit principles, procedures and methods
- knowledge of auditing management system standards
- skills to manage the audit programme

*Benedikt Heintel* was appointed as CAcert's internal lead auditor in CAcert's Committee motion m20131206.6. He is a professional auditor for Information Security Management Systems based on ISO/IEC 27001.

### 2.2.2 Auditor

An auditor is responsible for dedicated sessions during an audit. (S)He conducts interviews, does inspections, and observations to propose non-conformities or potential improvements to the organisation.

Auditors might be nominates for each audit plan separately.

### 2.2.3 Specialist

A specialist brings additional knowledge to the audit team without being an auditor. (S)He helps the auditor to understand systems and technologies and delivers the base for the auditor's decisions.

Specialists might be nominated session by session.

## 2.3 Extent of the audit programme

The internal audit over CAcert covers the organisation with is organs such as but not limited to

- the committee of CAcert Inc.,
- arbitration,

- policy group,
- support engineers,
- software development and assessment,
- projects,
- education including ATEs, Co-Audit, and CATS,

the Certificate Authority with its Registration Authority, and the technical infrastructure, i.e. data centres, servers, cabling, etc.

This audit programme has an extend of three years and contains three audit plans, one for each year. The audit plans specify the audited parts of CAcert. Within the three years, each and every part of the organisation should have been audited at least once.

The audit programme will take the results of former internal and external audits into concern.

All documentation will be done in English and published related on their severity based on CAcert's policies.

## 2.4 Risk evaluation

The audit programme follows a risk-based approach, taking into account the risk appearing in the context of planning, resources and selection of the audit team, communications, records and their controls, and the monitoring, review and improvement of this audit programme.

## 2.5 Audit procedures

Each audit under this programme follows the international norm ISO 19011:2011.

The lead auditor is responsible for the security and confidentiality of the information collected during the audit sessions. In her responsibility also lies the competence of the auditors, the selection of appropriate samples, the maintenance of the audit programme records, and the reporting to CAcert's committee.

# 3 Audit plan 2014

Table 3.1 contains all planned audit activities for the year 2014. Additional or ad hoc audit activities might be planned and integrated into this audit plan.

| **Area** | **Objective** | **Start** | **Involved Parties** |
|---|---|---|---|
| Arbitrated Background Check | Compliance | February 2014 | Arbitration |
| Arbitration | Deletion of an Assurer account | April 2014 | Arbitration |
| Assurances | Keeping CAP forms available | May 2014 | Arbitration, Assurer |
| Committee | Treasure, Secretary, Board Meetings | June 2014 | Committee |
| Software Development | Bug Tracking to deployment | July 2014 | Software Team |
| Critical | Critical infrastructure and team | October 2014 | Critical Admins |
| ATE | Training, Co-Audit | November 2014 | Education Team, AO, Co-Auditors |
| New Roots & Escrow Project | Audit over Test Root Creation | when possible | NRE Project Team |

Table 3.1: Audit Areas 2014

# 4 Audit plan 2015

Table 4.1 contains all planned audit activities for the year 2015. Additional or ad hoc audit activities might be planned and integrated into this audit plan.

| **Area** | **Objective** | **Start** | **Involved Parties** |
|---|---|---|---|
| CA/B Baseline Requirements | Compliance to the Baseline Requirements | | |
| Arbitrated Background Check | | | Arbitration |
| Arbitration | | | Arbitration |
| Assurances | | | Arbitration, Assurer |
| Committee | Treasure, Secretary, Board Meetings | | Committee |
| Software Development | | | Software Team |
| Critical | | | Critical Admins |
| ATE | Co-Audit | | Education Team, Co-Auditors |
| New Roots & Escrow Project | Escrow Test | if implemented | NRE Project Team |

Table 4.1: Audit Areas 2015

# 5 Audit plan 2016

Table 5.1 contains all planned audit activities for the year 2016. Additional or ad hoc audit activities might be planned and integrated into this audit plan.

| **Area** | **Objective** | **Start** | **Involved Parties** |
|---|---|---|---|
| CA/B Baseline Requirements | Compliance to the Baseline Requirements | | |
| Arbitrated Background Check | | | Arbitration |
| Arbitration | | | Arbitration |
| Assurances | | | Arbitration, Assurer |
| Committee | Treasure, Secretary, Board Meetings | | Committee |
| Software Development | | | Software Team |
| Critical | | | Critical Admins |
| ATE | Co-Audit | | Education Team, Co-Auditors |
| New Roots & Escrow Project | Escrow Test | if implemented | NRE Project Team |

Table 5.1: Audit Areas 2016