Distribution of board responsibilities

A collection of all current occurances of „board“ or „committee“ in the policies and a proposal how to distribute them in the context of the idea to add a „cabinet“ from Eva Stöwe

Assurance Area

Team management:

- appoint an Assurance Officer (AP 5, OAP 2.1)
- appoint Organisation Assurer (OAP 2.1)

Other decisions:

- grant additional Experience Points (AP 4.4)
- approve changes of “desert list” for TTP (TTPAssist 4.2)

Community / Wiki / Mailing lists:

- get report from Assurance Officer on all matters to do with assurances (AP 5)
- be notified on use of TTP outside of the desert list (TTPAssist 4.2)

Other decisions -> Arbitration

- Decide, where the OA is failing (OAP 2.1)
- Approve minor variations to TTPAssist by OA (TTPAssist 4.2)

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

PolicyOnPolicy (PoP)

During the period of DRAFT, CAcert Inc. retains a veto over policies that effect the running of CAcert Inc. (PoP 4.6.)

Does not make much sense, any more, as the running of CAcert Inc. would than governed by CAcert Inc. rules, only.

Maybe additionally or instead:

During the period of DRAFT, cabinet retains a veto over policies that effect the running of the critical systems. (PoP 4.6.)

(Or CA? which would be nearly everything?)

General change proposals:

Replace “Cacert Inc.” with “governing organization”, everywhere

Add in CCA 1: “governing organization: The governing organization is CAcert Inc.”

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

CertificationPracticeStatement (CPS)

Board or Cabinet?

- decide to add or remove accepted TLD Registrars on this list (CPS 3.1.7.)
- grant permission of use of the brand (CPS 9.5.2.)

Arbitration:

- documented and approved deviations of restrictions on members of audit team (CPS 8.3.)

Auditor may issue directives. Adequate discussion with Community (e.g., ~~CAcert Inc. Board~~ Cabinet and with Policy Group) should precede any directive (CPS 8.5.)

Change proposals:

1.3. PKI participants
CA is operated by the Community, managed by cabinet and under direction of (CPS 1.3.)

5.2.1. Trusted roles
Governance:

- Directors (members of the CAcert Inc. committee, or "Board")
- Cabinet
- internal Auditor
- Arbitrator

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

Dispute Resolution Policy (DRP)

- review, confirm or deny declaration of seal of case (DRP 3.2.)

~~The Board of~~ CAcert Inc. and the Members of the Community vest in Arbitrators full authority to hear disputes and deliver rulings which are binding on CAcert Inc. and the Members. (DRP 2.1.)

Change proposals:

3.5 Liability
The above [liability of Arbitrator] provisions may only be overridden by appeal process ~~(by means of a new dispute causing referral to the Board)~~. (DRP 3.5.)

Novel remedies outside the domain may be ~~routinely~~ confirmed ~~by the Board~~ by way of appeal process~~, in order to establish precedent~~. (DRP 3.6.)

4.2. The Disadvantages of this Forum
* Members may have their rights trampled over. In such a case, the community should strive to re-open the case ~~and refer it to the board~~. (DRP 4.2.)

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

Configuration-Control Specification

Hardware Control

Security Policy places executive responsibility for Hardware with the Board of CAcert Inc.

Access is delegated to Access Engineers (SP 2) and Systems Administrators (SP 3). Legal ownership may be delegated by agreement to other organisations (SP 9.4).

Software Control

Developers transfer full rights to CAcert (in a similar fashion to documents), or organise their contributions under a proper free and open source code regime, as approved by ~~Board~~ Cabinet.

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

SecurityPolicy I

Team management:

- approve changes about personal authorisation to list in SP 3.4 (SP 3.4.2., 7.1., 8.1., 9.1.1., 9.1.3., 9.1.5.)
- termination of access (staff) - also by resignation, Arbitration ruling, TL (SP 9.1.7.)

General management:

- responsible to the Community to manage the CA at the executive level. (SP 9.1.1., 9.3.1.)
- add additional components into Security Manual. (SP 1.1.)

Reports:

- get documentation from team leaders about emergency patch events (SP 3.2.3.1.)
- reported to by team leads (SP 9.1.2.)
- get regular reports about changes made to the system configuration (SP 4.1.3.)

Disaster recovery:

- End of management escalation chain for incident response (SP 5.3.3.)
- responsible for Disaster Recovery (SP 6.)
  - develop and maintain documentation on Business Processes (SP 6.1.)
  - identify Core Processes for business continuity / disaster recovery purposes (SP 6.1.)
  - identify standard process times and designate Maximum Acceptable Outages and Recovery Time Objectives for Core Processes. (SP 6.2.)
  - must have a basic plan to recover (SP 6.3)
  - maintain a Key Persons List (SP 6.4.)

Root keys:

  - Instruct root key generation & dual control (SP 9.2.1.)
  - control escrow of top-level roots (Subroots may also be escrowed by sys-admin team) (SP 9.2.2.)

Legal:

- Outsourcing of critical components must be approved by the Board (SP 9.4.)

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment

SecurityPolicy II

Change proposals:

> 9.3.2. Response to external (legal) inquiry
>
> All external inquiries of security import are filed as disputes and placed before the Arbitrator under DRP. ~~Board~~ Cabinet, CAcert Inc / governing organization and applicable team leaders must be notified.
>
> Only the Arbitrator has the authority to deal with external requests and/or create a procedure. Access Engineers, Systems Administrators, support engineers, ~~Board members~~ cabinet and its members, and other key roles do not have the authority to answer legal inquiry. The Arbitrator's ruling may instruct individuals, and becomes your authority to act.

Note:

This would allow / make it more explicit that the governing organization could answer on it's own, which could be problematic.

But the question is if mere policies could move this legal right away from a juristic person (the organization).

A better approach would be to make the organization to move such rights to arbitration which that organization has to accept, anyway.

Legend: cabinet committee of Inc arbitration community undecided irrelevant comment