# Participating in the Community

# Towards Audit

## The 1st Audit

- failed mid 2009
  - Primary reason:  lack of capacity
  - Deeper reason: “someone (else) is doing it.”
- Realisation that
  - *Auditor doesn't 'do' the audit*
  - *Board cannot 'do' the audit*
- Only **the Community** can muster the capacity

# Towards Audit

New strategy for audit

Many-part strategy:

1. Change the message
2. Build up the capacity...
3. Teams fix the problems
4. Engage an Auditor

# Towards Audit

Change the message from...

*“the board / auditor is doing the audit”*

To...

# Towards Audit

**YOU** are doing the audit!

# Towards Audit

## Example 1 – communications

*Ask not:*

When is my audit done for me,

*Rather, ask:*

What can I do for my audit?

# Towards Audit

## (easy) Example 2 - contributions

- Smaller audit checks → the Community.
- But, reliability for audit?
- Reliability comes from framework...
- We have the basics:
  - the CAP form!
  - the certificate!

# Towards Audit

CARS – CAcert Assurer Reliable Statement

To: Event Team Leader
I presented ATE material to _23_ Assurers
lang, CARS

# Towards Audit

- Add CARS to report
- Has meaning:

  *We the Community can RELY*

- Similar (same?) meaning as certs, CAP form
- Backed up by:  CCA, DRP
- team leaders can collate, reliably

# Towards Audit

## (harder) Example 3 - process

## Assurance Team is doing it's bit:

## Requirement:

*A.2.y The CP details how the CA verifies that*

*RAs operate in accord with CA's policies.*

# Towards Audit

## Solution:

*Education team creates the ATEs*

*Events team rolls it out to all Assurers,*

*Co-audit team checks the Assurers at each ATE,*

*Assurance Officer collects (CARS), collates, presents.*

*Here, today,*

you are contributing to the Audit!

# Helping CAcert?

## 2. Building the teams

i. Policy + Documentation + Internal Audit
ii. Assurance, Events, Education, Org-Assurers
iii. Dispute Resolution: Arbitrators + Case Managers
iv. Support: Triage + Support Engineers
v. Software: Testing, Development, Assessment
vi. Sysadm: Critical, Access, Infrastructure, Hosting

# Basics

Every role requires...

- ✔ Familiarity with the breadth and basics of CAcert.
- ✔ Assurer c.f., CARS.
- ✔ Helping with recruiting and training.
- ✔ Following Policies and Practices.

Some roles go through SP 9.2 process:

Arbitrated Background Check + Board approval

because of the access to data or special features.

# i. Consultants

Business Consultants lead Policies and practices to approval, and support Audit.

They are strongly aware of the policies and principles of the Community.
They are familiar with Security, IT standards and general business processes.

# ii. Senior Assurers

Senior Assurers help and run ATEs, develop the reach of Assurance, and develop the CATS Assurer Challenge.

They are very strong on Assurance. They are comfortable with people, presentations, and Community.

# ii. Organisation Assurers

Organisation Assurers verify Orgs.
They are good with org regulations,
careful and methodical.

They are strong on Assurance and
understand the needs of business.

# iii. Arbitrators

Arbitrators are people who show *exceptionally good judgement* in resolving difficult situations.

They are strongly aware of the policies and principles of the Community. Good at listening, researching, thinking, reducing and writing.

# iii. Case Managers

Case Managers are organised, good with detail, on top of email, and comfortable with working to the tune of the Arbitrator.

And, they do not fall in the trap of letting their opinions carry them away.

# iv. Support Engineers

Support Engineers are people with lots of time, able to communicate with humans and techies.
SEs are very patient, cautious and reliable.
SEs are “completers,” very methodical.

SP: ABC+approval

# iv. Triage

Triage have:

- some time, daily,
- comfortable with webapps (OTRS),
- able to quickly dive into messy emails,
- and slice and dice them to the right place.

Triage is the starting place for a lot of things...

# Software

**New**: larger architecture + design
(later) mix of Java, PHP, Javascript, C/C++ likely.
**Old**: patience with old, undocumented PHP.
And a desire to get us back on track with fixes!
**Testers**: patient, communicative with techies
and can see the human/user view.

**Software Assessors**: approve changes

SP: ABC+approval.

# Infra Team

Infrastructure Sysadms are very good with Linux, and know quite a lot about security practices.

Because of our need for 4 eyes and dual control and redundant access to our systems, all sysadms work with 1-3 others in small teams. Follow doco, share brief reports on actions.

# Access Engineers

Access Engineers:  located near Ede, NL.

Strongly familiar with security access controls and with basics of hardware and hosting.

Watches for proper procedures and controls. Follows Security Policy, records actions.

SP: ABC+approval.

# Critical Sysadms

The systems administrators on the critical team work to Security Policy (“the bible”) and other documentation.

Strongly familiar with security.  Always working with at least 1 other under 4 eyes or dual control. Follows Security Policy, records actions.

SP: ABC+approval.

# Helping CAcert?

## Building the teams (redux)

i. All of these teams exist
ii. More info in January's Annual Report

svn.cacert.org/CAcert_Inc/General_Meetings/AGM-20100130/CAcert_Annual_Report_2009.pdf

iii. 13 teams, 28 pages, 20 cats, 3 kangaroos...
iv. Straw poll: 3+4+5+5+4+2+4+5+6+2 = **39**
v. No invitation, just ask...

# Towards Audit

## What can I do for my audit?