CAcert und das Audit

1. CAcert und das Audit (Übersicht)

2. CAcert Businessbereiche

a. Audit und Assurance

b. Audit und Systeme

c. Audit und die Community

3. Audit Prolog - Ausblick

1. CAcert und das Audit

- Um CAcert Root-Zertifikate in Browser zu bekommen
- => wird ein Audit benötigt
- => das erfordert
  - Management
  - Policies + Verfahrensanweisungen
  - Audit der Geschäftsabläufe & Systeme
- => gegenüber diesen Richtlinien und Verfahren.

1. CAcert und das Audit

- CAcert hat drei wesentliche Business Bereiche
  - Assurances
  - Systeme
  - Community

1. *CAcert und das Audit (Übersicht)*
2. **CAcert Businessbereiche**
   a. **Audit und Assurance**
   b. *Audit und Systeme*
   c. *Audit und die Community*
3. *Audit Prolog - Ausblick*

2.a. Audit und Assurance

2.a. Audit - Assurance

a. Assurance

- Assurance Policy ist nun in
  => vollem POLICY-Status
- **Verbindlich** für alle Assurer
- Der Prozess der Assurance kann nun geprüft werden.

2.a. Audit - Assurance

a.i Drei wichtigen Prozesse für das Audit

- CATS – Assurer Challenge (Training, Prüfung)
- Assurer Training Event
- co-Audit

2.a. Audit - Assurance

CATS Assurer Challenge

- CAcert Automated Testing System
- 25 Multiple Choice Fragen,
  80% müssen richtig beantwort werden
- Du kannst so es so oft probieren wie du es willst
- Setzt einen Minimal Standard
- Erste Challenge: Login mit Client Zertifikat

2.a. Audit - Assurance

Assurer Training Event

- ATE findet heute statt!
- 20 bislang in Europa

  Deutschland, Niederlande, Innsbruck, Paris, London, Prag, Budapest
- Informiert dich, worüber du bescheid wissen sollst
- Besonders Empfohlen

2.a. Audit - Assurance

Co-Audit

- Assurer sollen Auditor prüfen
- Beleg für Assurance im Einklang mit der Policy
- verifiziert die Qualität der Assurance

  “A.2.y CP beschreibt detailiert wie die CA das überprüft: RA operiert gemäß CA's Policies.” (CP ≙ CPS)

- (Ebenso: reichlich Feedback)

2.a. Audit - Assurance

a.ii Details der Änderungen bzgl. Assurance

- Mitglieder Zustimmungen:
  “Information ist korrekt”
  “Ich akzeptiere die CCA”
- Assurer Bestätigung:
  “Assurance erfolgte nach Assurance Policy”
- CARS: CAcert Assurer Reliable Statement
  (CAcert Assurer - überprüfbare Bestätigung)

2.a. Audit - Assurance

a.iii Die Überprüfung der Assurances

✓ 2009 Februar – Juni: Überprüfung durch Auditor

✗ Audit wurde aus anderen Gründen abgebrochen.

- Möglichkeit der Überprüfung der Assurance Herbst 2010

1. *CAcert und das Audit (Übersicht)*
2. **CAcert Businessbereiche**
   a. *Audit und Assurance*
   b. **Audit und Systeme**
   c. *Audit und die Community*
3. *Audit Prolog - Ausblick*

2.b. Audit und Systeme

2.b. Audit - Systeme

b.i Systeme Audit nötig

- Sicheres Hosting: Oktober 2008
  (Teams, Gebäude, Maschinen)
- Security Policy: März 2009 p20090327
- Software
  (CPS: Juli 2009 p20090706, Teams)

2.b. Audit - Systeme

b.ii Systeme haben nun …

- Teams: Critical Sysadmins, Access Engineers
- Security Policy im DRAFT-Status

  => Verbindlich für kritische Rollen:
  Systemverwalter und
  Zugangskontrolleure

- Systeme im Sicheren Rechenzentrum:
  BIT Ede, NL

2.b. Audit - Systeme

b.iii Problemlösungen

- Non-Critical Systems – in Arbeit
- Roots – in Planung
- Disaster Recovery – in Entwicklung
- Team Größe – es werden mehr Leute benötigt

2.b. Audit - Systeme

b.iv Software

- Überprüfung Innsbruck April 2009

„Ernsthafte Schwierigkeiten bei der Wartung, Optimierung und Absicherung”

„keine verläßliche Aussage möglich.”

- Weg 1: Neues Software Entwicklungsteam, neues Design, Neuaufbau: “BirdShack”
- Weg 2: Alte Software in „Maintenance Mode”

1. *CAcert und das Audit (Übersicht)*
2. **CAcert Businessbereiche**
   a. *Audit und Assurance*
   b. *Audit und Systeme*
   c. **Audit und die Community**
3. *Audit Prolog - Ausblick*

2.c. Audit und die Community

2.c. Audit - Community

- Das Audit Kriterium:

  DRC für "David Ross Criteria".

- David ist ein Qualitäts-Ingenieur im Ruhestand
- Er startete das CAcert Audit
- Er hat eine andere Aufgabe übernommen

2.c. Audit - Community

DRC hat eine solide Grundeigenschaft:

die verlangen, das

- Risiken,
- Haftung, und
- Pflichten

  jedem offengelegt werden!

2.c. Audit - Community

Dies errichtete etliche gewaltige Hürden für die CA:

- Was genau sind die Risiken/Haftung/Pflichten?
- Auf wen beziehen sie sich?
- Sind sie zumutbar?
- Und wie gehen wir mit ihnen um?

2.c. Audit - Community

Die Barrieren der R/H/P sind subtil:

- DRC sagt nicht dabei fair zu sein,
- lässt aber die Freiheit zu, das zu betrachten
- CAcert Leute wünschen aber das es fair zugeht

  d.h. Wir müssen damit umgehen!

2.c. Audit - Community

Ein wichtiges Ergebnis der Überlegungen war wir benötigen eine

Vereinbarung der CAcert Gemeinschaft

➔ CAcert Community Agreement

und sie muß folgendes leisten ...

2.c. Audit - Community

Die CCA hat dabei folgende Aufgaben:

a. die Mitglieder in eine beidseitig verpflichtende Gemeinschaft einzubinden

b. die Risiken/Haftung/Pflichten festzulegen.

c. die Haftung zu begrenzen → 1000 Euro

d. die Haftung zuzuweisen →
zurück an die Mitglieder

2.c. Audit - Community

Wie können wir die Haftung zuweisen?

- Durch unser eigenes „Forum der Streitbeilegung“
  “Arbitration”
- Zustimmung dieser Form der Streitbeilegung
  CAcert Community Agreement 3.2
- Schreiben einer Policy zur Kontrolle des Prozesses

  Dispute Resolution Policy

2.c. Audit - Community

Zusammenfassung:
Das „Warum“ einer Arbitration geht darauf zurück

- Audit (DRC) zwingt die Offenlegung der Haftung
- Einfacher Fix: *Limitierung*
- Komplexer Fix: *Zuweisung*
- die sichere und günstige Lösung der Zuweisung:

  eine eigene Arbitration nutzen

(Das letzte Kapitel diskutierte das „Wie“.)

1. CAcert und das Audit (Übersicht)
2. CAcert Businessbereiche
   a. Audit und Assurance
   b. Audit und Systeme
   c. Audit und die Community

3. Audit Prolog - Ausblick

3. Audit Prolog / Ausblick

3. Audit - Vergangenheit

Audit lief Anfang 2009 auf Hochtouren, aber aufgrund

- Mangelnder Kapazitäten
- Zeitüberschreitung
- Fehlender Geldmittel

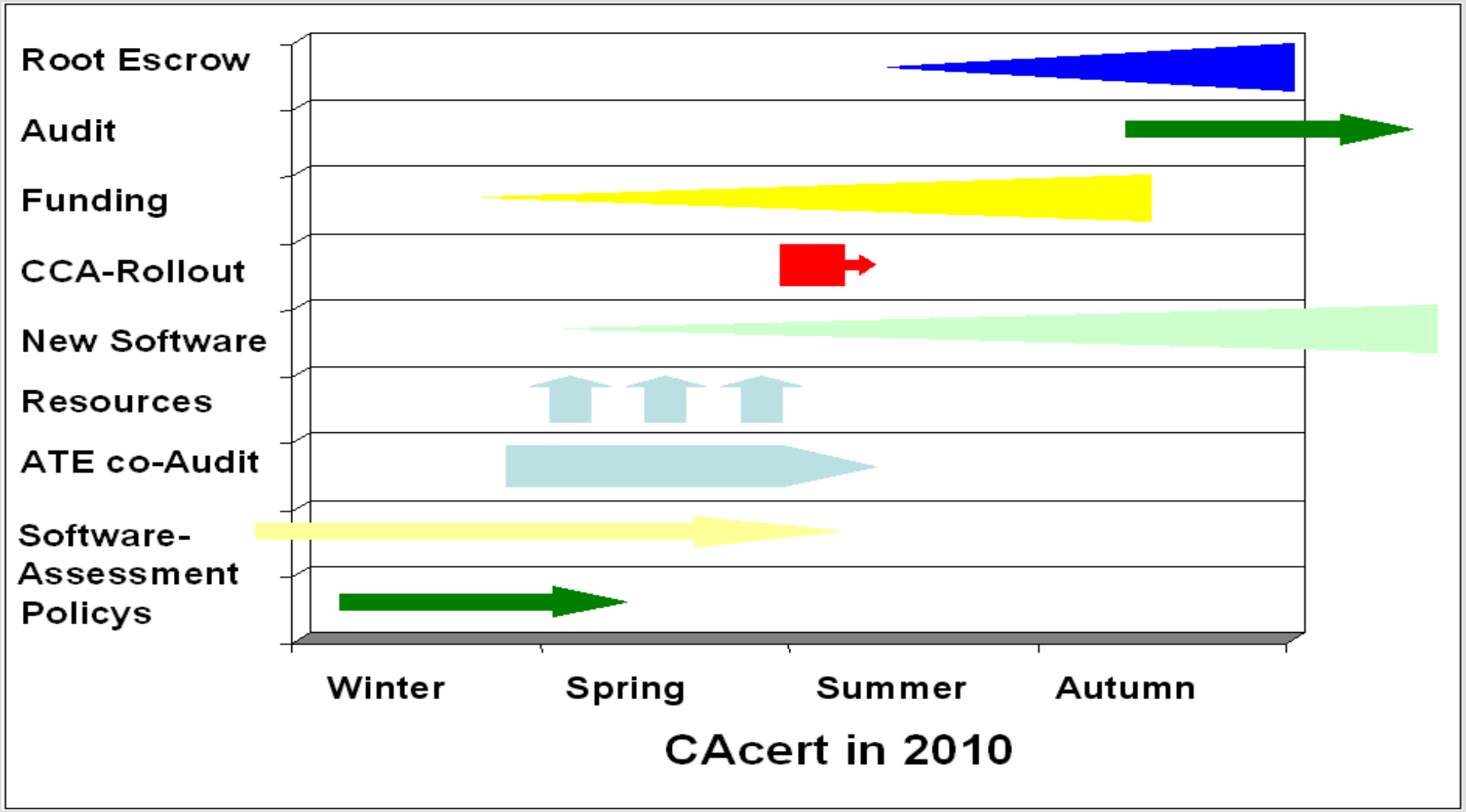
stoppte das Audit im Juli 2009

3. Audit - Zukunft

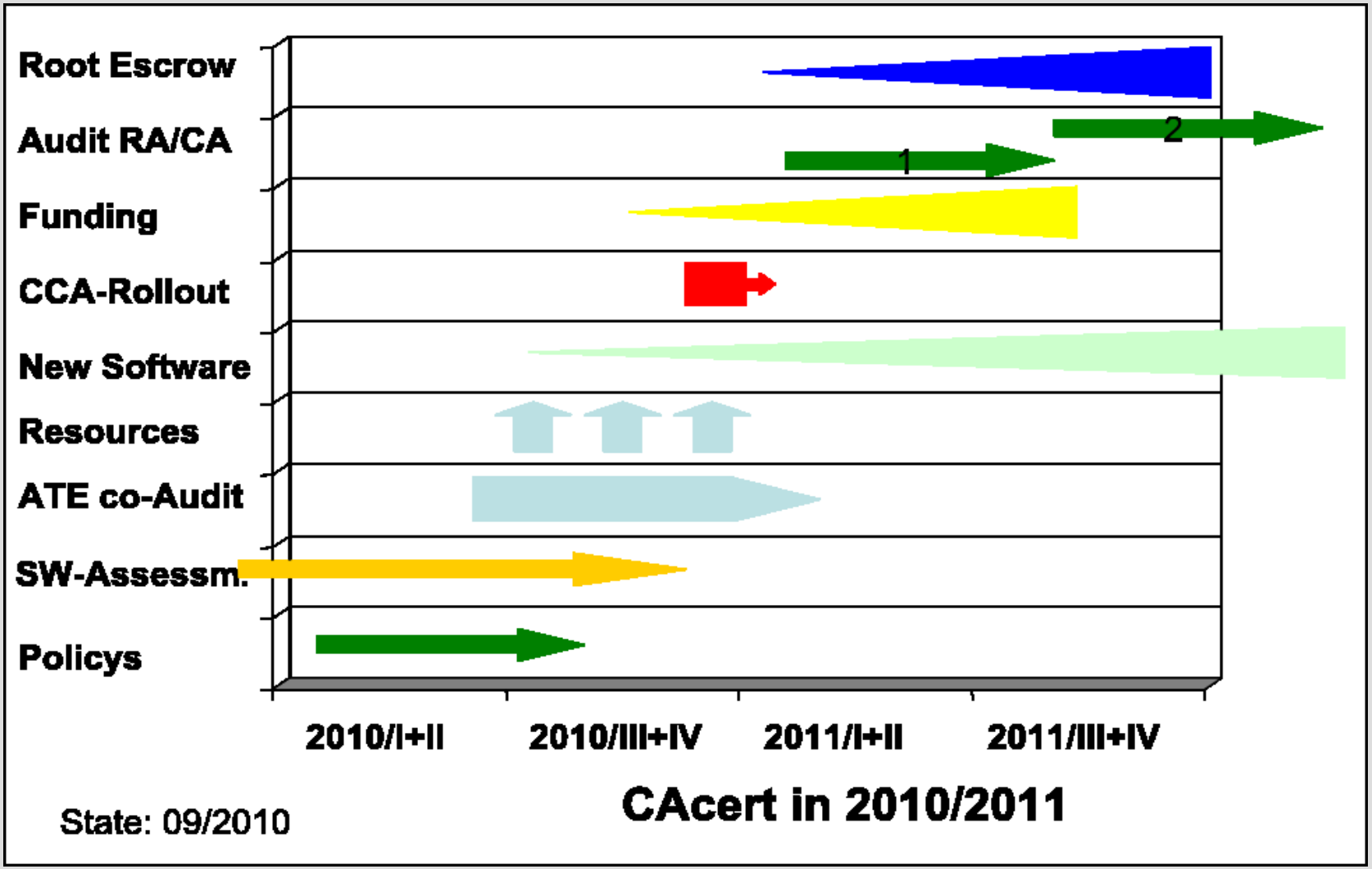
Welche Aufgaben stehen für die Community an?

- Rebuild Software
  so wie mit: Assurance, Arbitration, Support, Systeme, Management
- Audit Aufgaben in die Community zu übertragen
  Nur die Community kann skalieren und hat die Möglichkeit
- Bereit zum Audit über die Assurance
  Heute ist deine Chance: ATE!
- Geldmittel Beschaffung!

Inoffizieller CAcert Plan 2010 (Jan 2010)



Inoffizieller CAcert Plan 2010 (Sep 2010)



1. CAcert und das Audit (Übersicht)
2. CAcert Businessbereiche
   a. Audit und Assurance
   b. Audit und Systeme
   c. Audit und die Community
3. Audit Prolog - Ausblick

CAcert und das Audit

Fragen ?