Enabling Efficient, Consistent Certification and Accreditation Enterprise-Wide

Overview

- Certification & Accreditation
- The IRS Challenge
- The Solution: Xacta Web C&A
- Where Are We Today?
- Future Direction
Certification and Accreditation (C&A)

The Process Defined

- **Certification**
  - Analyze system threats and vulnerabilities
  - Analyze system security features
  - Analyze and document ‘residual risks’

- **Accreditation**
  - Accept risk
  - Grant authority to operate

Why C&A?

- **It’s the Law!**
  - Compliance is mandated government-wide

- **It Makes Good Sense**
  - Gain an understanding of a system and its interaction with other systems
  - Improve system security

- **It Requires**
  - Periodic review of existing systems
  - That modified and new systems must be accredited before they “go live”
Standardized C&A Processes

- **DITSCAP**
  - Standard C&A process for Department of Defense

- **NIACAP**
  - Standard process for other federal departments and agencies
  - Virtually identical to DITSCAP

- DITSCAP and NIACAP work well with *any* departmental or agency security requirements

IRS Challenge

*Improve the C&A process*

- Existing C&A process too lengthy
- Existing C&A process too resource-intensive
- Results not consistent: documentation “out of sync” with reality
- Meaningful management information not available
IRS Goal: Integrated Approach

- Compliance with NIACAP and IRS-specific regulations, policies, procedures and standards
- Automated, consistent, repeatable process
- Status information available to management
- Standardized document content quality
- Central repository for certification data
- “One button” publishing with automated formatting

IRS Development Process

- Market research on C&A tools
- “Make vs Buy” decision
- Thorough understanding of product
- Re-engineer current C&A process
- Develop and document IRS-specific training, system administration, workflow
- Conduct awareness, system administration and end-user training
- Ensure coaching/hand-holding of users on pilot C&A projects
The Solution: Xacta Web C&A 2001

Automates C&A Processes/Compliance

• Provides organized method of collecting system information
• Includes extensive knowledge base consisting of:
  - National, departmental, and agency-level security regulations
  - Comprehensive security testing and evaluation methods and procedures
• Automatically generates SSAA & appendices

The Solution: Xacta Web C&A

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually enter HW/SW information</td>
<td>Use Detect functionality to automatically map HW/SW information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard copy security library highlighting applicable regulations</td>
<td>Built-in content libraries, automated identification of applicable regulations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual development of test procedures and checklists</td>
<td>Automated checklists and recommended test procedures</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple word processing applications, managing fonts, tabs, formats, etc.</td>
<td>One-button publishing, automated formatting, consistent output across systems</td>
<td></td>
</tr>
</tbody>
</table>
The Solution: Xacta Web C&A

Stage 1: Information Gathering
Stage 2: Requirements Analysis
Stage 3: Testing
Stage 4: Risk Assessment
Stage 5: Publishing

The Solution: Xacta Web C&A

- Enables consistent, cost-effective C&As
- Generates complete, high quality output efficiently
- Reduces reliance on security experts/outsourcing
- Promotes security policy across enterprise
- Provides system-of-systems view of C&A status and vulnerabilities
- Focuses remediation efforts to improve risk posture on an on-going basis
Where are we today?

**Internal Revenue Service:**
*Realizing the Vision*

- Purchased Xacta Web C&A from Telos Corp.
  - Enterprise Subscription Agreement
  - ~600 systems to C&A
  - Content customized for IRS policy and regulations
- Utilizing Xacta mentoring services for initial C&As
- Contracting for CBT and train-the-trainer
- Implementing consistent, reliable C&A process
- Administering security policy across organization
- Making security assessment an integral part of the IRS business process

---

**Where are we today?**

**IRS C&A Process**

- Stage 1: Information Gathering
- Stage 2: Requirements Analysis
- Stage 3: Testing
- Stage 4: Risk Assessment
- Stage 5: Publishing

KICK-OFF MEETING
TEST
REVIEW & EVALUATE
RECOMMEND CERTIFICATION
CERTIFY & ACCREDIT
POST ACCREDITATION
Where are we today?

---

**Internal Revenue Service: Lesson Learned**

- Re-engineering the C&A process as we automate it is a difficult task
- Automating the workflow is difficult when roles and responsibilities are still being worked out
- System administrative setup required substantial resources
- A great deal of initial “hand-holding” is required
- Participation by all stakeholders is necessary to successfully complete a C&A project
- **THIS IS AN ONGOING EFFORT – WE ARE CONTINUALLY LEARNING!**
Future Direction

**Internal Revenue Service:**
*Future plans for Xacta Web C&A*

- Identification of an agency-wide network of coaches for Xacta Web C&A projects
- Self-use by end users
- Charge-back to Business Owners by 2004

---

**Going Beyond Compliance**

**Xacta Web C&A 2002**

- Information regarding configurations, vulnerabilities, events, adherence to process and policy
- Response to events, vulnerabilities, and compliance issues
- Continuous feeds, via the Internet, of most up-to-date patches, alerts, bulletins…
Going Beyond Compliance

Compliance vs Continuous Risk Assessment

Continuous Risk Management Approach

Questions?

You Can Rest Easy
With a Strong Security Program

You Can Rest Easy