How Auditors Certify Systems
A Look at 3rd Party, Non-Vendor, Legally Mandated System Certifications

OWASP Toronto

February 16. 2011
Toronto, Ontario

Jerrard B. Gaertner
CA•IT/CISA, CISSP, CGEIT, CIPP/IT, I.S.P., CIA, CFI
Soberman Technology Assurance Inc.
Soberman LLP
jgaertner@soberman.com

1

Introductions

2

1

Jerrard Gaertner

- **Director, STAI**
- **Executive Vice President – CIPS**
  (Canadian Information Processing Society)
- **CA w/ specialist designations**
  - **CGEIT, CISSP, CIPP/IT, CIA, CFI, I.S.P., ITCP… (yawn)**
- **25+ years experience in systems assurance, IT controls and related areas**

SOBERMAN LLP (C) 2011   3

Soberman Technology Assurance Inc.

- **Subsidiary of Soberman LLP**
- **Technology governance**
- **GRC for IT**
- **Computer controls and security**
- **Privacy risk and statutory IT audits**
- **Specialized engagements – PCI, CICA 5970, SAS 70, digital forensics and data capture**

SOBERMAN LLP (C) 2011   4

Agenda

- **Types of system certification**
- **Why and when are system certifications required?**
- **Who can perform a system certification**
- **Standards and approach**
- **More "important" certifications**
- **Be Aware!**
- **Preparing for a certification audit as an IT professional**
- **Q & A**

Types of System Certification – Legal Foundations

- **Statutory or non-statutory**
  - **FIPS 140-2; OMB Cert & Assess; IEEE vs. PCI, Cisco, Verisign**
- **Regulatory or non-regulatory**
  - **52-109; SOx vs. SAS 70, CICA 5970**
- **Contractual or ad hoc**
  - **PCI; SAS 70 vs. Systrust, SAS 70**
- **Vendor or non-vendor**
  - **Cisco; Verisign vs. CObIT, ITIL**

Types of System Certification – Legal Foundations

- **Commercial/for-profit or professional/NFP**
  - *Webtrust; Truste, Verisign vs. ISO, ITIL, ISACA*
- **Owner initiated or 3rd party initiated**
  - *CICA 5970, ISO, Cisco, Webtrust vs. PCI, SCADA, SOx*

Types of System Certification – Subject Matter

- **System operates reliably – uptime, accuracy, reproducibility**
- **System data is secure and/or private**
- **Backup and recovery capability**
- **System data is proof against financial manipulation**
- **System complies with specified standards (technical or otherwise)**
- **System controls are adequate to provide reasonable assurance that…**

Types of System Certification – Issuers and Originators

- ISO
- ITIL
- CICA
- AICPA
- OSC
- IBM
- Cisco
- Microsoft
- SANS Institute

Types of System Certification – Issuers and Originators

- ISC(2)
- ISACA
- Governments (FIPS, OMB)
- PCI Council
- NIST
- Verisign
- Symantec
- ….

Why and When are Certifications Required?

- **When there is a need to have *independent* assurance of performance, standards, security, compliance, controls…**
  - Segregation of duties, self-evaluation, conflict of interest
- **When multiple parties are reliant on a system or application and individual audits are no longer practical**

SOBERMAN LLP (C) 2011   11

Why and When are Certifications Required?

- **When special training is required to perform certification and in-house assurances and expertise are insufficient for third parties**
  - In-house expertise in operations, not applicable standards or audit work
  - Auditors have a fiduciary duty to others (not the employer or system owner under review)

SOBERMAN LLP (C) 2011   12

Why and **When** are Certifications Required?

- **As required by statute, regulation, contract, business requirements, custom**
- **As reliance on third parties (hosting, Saas, development… exceeds a comfort, materiality or regulatory threshold**
- **As systems become certifiable (ready to be audited)**
- **As resources become available to (a) pay for and (b) support in house the necessary audit work**

SOBERMAN LLP (C) 2011   13

Who Can Perform a System Certification?

- **General standards**
  - **Adequately trained and experienced**
  - **Objective and independent**
  - **Appropriately accredited**
  - **Sufficient time, resources, access**
- **Specific standards**
  - **Depends on the nature of the certification**
  - **Licensing requirements - must be recognized by the certifying body**

SOBERMAN LLP (C) 2011   14

Who Can Perform a System Certification?

- ISO auditors
- SCAD auditors
- PCI Qualified Sec Assessor
- ITIL auditors
- CA/CPA designated auditors
- CISSPs
- I.S.P.s
- "Privacy by Design" registered auditors
- ….

SOBERMAN LLP   (C) 2011   15

Standards and Approach

- **Prescription or descriptive standards**
  - PCI DSS; FIPS 140-2 vs 52-109; CICA 5970
- **Fixed scope or flexible scope**
  - ANSI, OMB Cert & Assess; ISO vs Cobit, SAS 70, Webtrust
- **Mechanistic or professional judgment**
  - PCI DSS; Cisco vs ITIL; CICA 5970

SOBERMAN LLP   (C) 2011   16

8

Standards and Approach

- CICA/AICPA
- ISO
- ITIL
- CObIT/ISACA
- IIA
- PCI
- NIST
- ANSI/IEEE
- Microsoft
- ….

SOBERMAN LLP (C) 2011   17

More "Important" Certifications

- For specific assurance provided to defined third parties with respect to systems compliance – mostly financial related
  - CICA 5970
  - AICPA SAS 70
- For the right to process credit cards
  - PCI

SOBERMAN LLP (C) 2011   18

9

More "Important" Certifications

- **For the right to sell to high security, US government purchasers and for marketing purposes to the public**
  - **FIPS 140-2**
- **For operational excellence in IT**
  - **ITIL**
  - **ISO**
- **For web presence**
  - **Verisign**

More "Important" Certifications

- **CICA/AICPA Certifications**
  - **Non prescriptive**
  - **Control objectives selected by auditee and intended audience (not fixed)**
  - **Control techniques sufficient to meet objectives (professional judgment)**
  - **May or may not use recognized framework (i.e. CObIT)**
  - **Originated as financial/service bureau certification**

More "Important" Certifications

- **CICA/AICPA Certifications**
  - **2 flavours – point in time and continuous**
  - **Annual audit or more frequently**
  - **Often mandated by major customers and trading partners of auditee**
  - **Must be performed by a CA/CPA firm**
  - **Supporting audit work may be quite limited**
  - **Often misinterpreted by readers**

SOBERMAN LLP (C) 2011 21

More "Important" Certifications

- **PCI**
  - **Highly prescriptive**
  - **Narrowly focused (security of credit card information and processing)**
  - **If auditee unprepared, can lead to costly, high pressure remediation efforts**
  - **Annual audit or more frequently**
  - **Multiple flavours – payment systems, payment applications, scanning vendors**

SOBERMAN LLP (C) 2011 22

11

More "Important" Certifications

- **PCI**
  - **Multiple flavours – rigour of audit determined by number of transactions processed**
  - **Must be performed by QSA, although can have internal QSA**
  - **Limitation of liability and transference of risk**

SOBERMAN LLP (C) 2011

23

Be Aware!

- **Top Reasons Certification Audits Fail**
  - **Poor planning and preparation**
  - **Policies, procedures and training not adequately documented/addressed**
  - **Corporate culture not security-oriented**
  - **Inadequate understanding of expectations of auditors**
  - **Poor communications between stakeholders (IT, security, management, auditors)**

SOBERMAN LLP (C) 2011

24

Be Aware!

- **Top Reasons Certification Audits Fail**
  - **No (inadequate) security and control framework in place in IT**
  - **No provision for follow up, exception reporting and enforcement**
  - **Fundamental flaws in system architecture**
  - **Over-reliance on encryption or other "secure" technology**

SOBERMAN LLP (C) 2011   25

Be Aware!

- **Top Reasons Certification Audits Fail**
  - **Forgetting about application and data base controls**
  - **Poor configuration management**
  - **Poor segregation of duties**
  - **Inability to articulate relevant compensating controls**

SOBERMAN LLP (C) 2011   26

13

Be Aware!

- **Passing one audit does NOT mean passing another of a different type**
- **Passing one audit does NOT mean passing the same audit at a later date – even if nothing changes**
- **Terms of reference of an audit can change, based on findings. Never assume that something apparently out of scope is irrelevant**

SOBERMAN LLP (C) 2011   27

Be Aware!

- **Audit testing can be either an analog or a digital function**
  - **If 9 times out of 10, incident response time is below 5 minutes and one time it is 7 minutes – that is probably a "pass"**
  - **However, if even one suspicious access is not followed up, that may well constitute a "fail".**
- **"Doing it" is not enough – you have to be able to prove that you "do it"**

SOBERMAN LLP (C) 2011   28

14

Be Aware!

- **"We don't have enough staff" is never an excuse**
- **Helping the auditors IS a better strategy than hindering or ignoring them**
- **It is almost always better, cheaper and less stressful to fully prepare for an audit in advance, than remediate and be re-audited!**

SOBERMAN LLP   (C) 2011   29

Preparing for a Certification Audit as an IT Professional

- **Understand the scope, standards, framework and requirements of the audit!**
- **Perform a self-assessment early on to identify possible weaknesses**
- **Enlist assistance from internal audit, application users, corporate management as required**
- **Perform a pre-audit if unsure of current status and readiness (either internally or preferably using a qualified auditor)**

SOBERMAN LLP   (C) 2011   30

Preparing for a Certification Audit as an IT Professional

- **Review documentation (policies, procedures, internal standards) for applicability**
- **Prepare an information package to help orient the auditor**
- **Ensure that logs, exception reports and other evidence are retained on a meaningful schedule**
- **Consider the results of other (previous) audits**

SOBERMAN LLP (C) 2011   31

Preparing for a Certification Audit as an IT Professional

- **Prepare IT staff – try to create a culture of cooperation among the IT staff (not confrontation)**
- **Become familiar with relevant best practices and implement as possible**
- **Where remediation is not immediately possible, have a remediation plan, including time frame, available to show the auditor**

SOBERMAN LLP (C) 2011   32

16

# Get Stakeholders Involved in the Pre-Audit Process

33

Some BEST Practices

- Separate GOVERNANCE committee composed of senior user, IT and executive management responsible for strategic decisions and ensuring that the proper controls and safeguards are in place to ensure the project's success
- Implement ITIL, COBIT, quality-centric application life cycle management processes (as applicable)
- Invest in appropriate IT staff training
- Create a culture of quality development and pride in work
- Ensure consistency and knowledge transfer through standards and documentation and enforce them

34

17

Some BEST Practices

- **Invest in monitoring and productivity tools**
- **Use risk assessment to increase the likelihood of success**
- **Don't act by rote – re-examine procedures and methods and invoke a continuous improvement paradigm**
- **Institute METRICS – if it can't be measured it can't be managed!**
- **Be transparent in communications and management**
- **Be prepared to escalate if an issue is not be addressed**

SOBERMAN LLP (C) 2011   35

That's all for now

SOBERMAN LLP (C) 2011   36

18
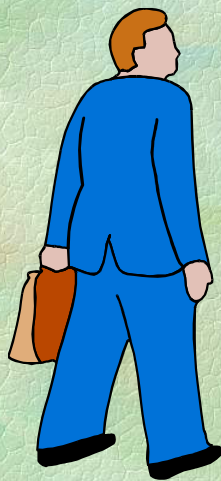
Questions?
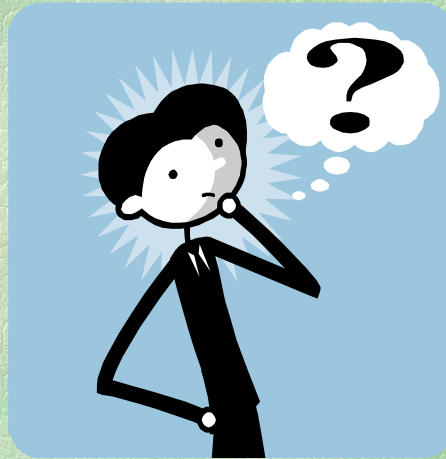
Contact Information

Jerry Gaertner

Soberman LLP and
Soberman Technology Assurance Inc.
2 St. Clair Avenue E., Suite 1100, Toronto
416-963-7192
416-505-0307 (c)
jgaertner@soberman.com