The Role of Pen Testing and Application Scanning as Part of an Enterprise Information Systems Risk Management Framework

Selling the Value of Your Work at the Executive Level

James Connolly CISSP, CISA, MBA

Agenda

- Defining Terms
- What every CIO wonders
- How your results help the CIO answer that question
- Root Cause
- Extrapolation
- Feed back to improve processes that led to bad outcomes

Defining Our Terms

Committee on National Security System
CNSS Instruction No. 4009 26 April 2010
National Information Assurance (IA) Glossary

- risk management The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program.
- NIST SP 800-53: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system, and includes: 1. the conduct of a risk assessment; 2. the implementation of a risk mitigation strategy; and 3. employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- Risk Management Framework (RMF) A structured approach used to oversee and manage risk for an enterprise.
- penetration testing A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

www.cnss.gov/Assets/pdf/cnssi_4009.pdf

COBIT Definition: IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains

- Furthermore, IT governance integrates and institutionalises good practices to ensure that the enterprise's IT supports the business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission's (COSO's) *Internal Control—Integrated Framework, the widely accepted control framework for enterprise governance and risk management, and similar compliant* frameworks.
- Organisations should satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management should also optimise the use of available IT resources, including applications, information, infrastructure and people. To discharge these responsibilities, as well as to achieve its objectives, management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide.
- *Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process* framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts.
- They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

COBIT 4.1

Your Best effort or industry best practice which would you rather defend as an exec

IT Governance Institute wishes to recognise:
Expert Developers and Reviewers

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA	Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK	Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium	Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA	Gary S. Baker, CA, Deloitte & Touche, Canada	David H. Barnett, CISM, CISSP, Applera Corp., USA	Christine Bellino, CPA, CITP, Jefferson Wells, USA	John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK	David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA	Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium	Don Canilglia, CISA, CISM, USA	Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina	Boyd Carter, PMP, Elegantsolutions.ca, Canada	Dan Casciano, CISA, Ernst & Young LLP, USA	Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore	Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA	Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA	Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA	Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA	Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA	Peter De Bruyne, CISA, Banksys, Belgium	Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium	Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium	Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA	Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA	Zama Dlamini, Deloitte & Touche LLP, South Africa	Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand	Troy DuMoulin, Pink Elephant, Canada	Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA	Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay	Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland	Christopher Fox, ACA, PricewaterhouseCoopers, USA	Bob Frelinger, CISA, Sun Microsystems Inc., USA	Zhiwei Fu, Ph. D, Fannie Mae, USA	Monique Garsoux, Dexia Bank, Belgium	Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA	Guy Groner, CISA, CIA, CISSP, USA	Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium	Gary Hardy, IT Winners, South Africa	Jimmy Heschl, CISA, CISM, KPMG, Austria	Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA	Tom Hughes, Acumen Alliance, Australia	Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia	John A. Kay, CISA, USA	Lisa Kinyon, CISA, Countrywide, USA	Rodney Kocot, Systems Control and Security Inc., USA	Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium	Linda Kostic, CISA, CPA, USA	John W. Lainhart IV, CISA, CISM, IBM, USA	Philip Le Grand, Capita Education Services, UK
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA	Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA	Debbie Lew, CISA, Ernst & Young LLP, USADonald Lorete, CPA, Deloitte & Touche LLP, USA	Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA	Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA	Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK	Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia	Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK	Anita Montgomery, CISA, CIA, Countrywide, USA	Karl Muise, CISA, City National Bank, USA	Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA	Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA	Ed O'Donnell, Ph.D., CPA, University of Kansas, USA	Sue Owen, Department of Veterans Affairs, Australia	Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa	Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA	Vitor Prisca, CISM, Novabase, Portugal	Martin Rosenberg, Ph.D., IT Business Management, UK	Claus Rosenquist, CISA, TrygVesata, Denmark	Jaco Sadie, Sasol, South Africa	Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia	Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA

How do you explain what a framework is?

You are going to climb Mt Rainier. what should be in your back pack?

- wing it
- ask your brother-in-law, he did it once
- go the Mt Ranier Climbing Association's web site and download the list they have been maintaining for the last 20 years

A framework is the collective work of industry experts to describe the controls that should be in place to reliably manage the activity

three good things about that

- is reasonable and prudent to rely on the work of those experts
- It organizes the controls into collectively exhaustive and mutually exclusive to facilitate review
- It creates a common language for people inside and outside the organization to discuss controls

What Every CIO should wonder

- Every CIO asks the question “Am I doing enough?”
- Smart CIOs as the question how can I credibly respond to the question “Am I doing enough?” and have the answer be yes.

There probably something wrong. How are you going to find it.

- It breaks
- A hacker finds it for you
- The Wall Street Journal
- An unsatisfactory audit
- You can pay for good testing

In any case it has to be fixed

The difference is what it does to your reputation and how much control you have over the response

Before you start

- Can you get the assets that you are looking for in context of the enterprise the same way the CIO does
- Use inventory or risk rating to target your work where it has the most impact.

  Understand Business Function or Information Classification to help deliver impact statements if something is wrong

  Business Impact Value Analysis

  What goes wrong when C, I, A, O are breached for all information classes stored on or transformed by the asset/application

Once you find something wrong

- Remember, fixing this instance of the problem is just the start of the value chain, keep going up.
  - What process should have been in place to prevent or detect that
    - Change management
    - Patch Management
    - Application Development Training
    - Pre Implementation testing
  - Identify a process within a recognized framework should have been operating effectively to prevent that error
  - Extrapolate the results across the enterprise of that control not being effective
  - Recommend evaluation of that control against industry guidance

  - Your work identifies weaknesses in the control environment that the CIO is accountable for designing and operating effectively, and gives them the opportunity to make improvements to those controls in a deliberate and planned manner, and support the statement that they are using an industry framework to evaluate and prioritize improvements to the IT governance

Next step up the value chain

- Ask what management is afraid of
  - Look to framework to see what controls should be in place to reduce the likelihood that is happening
  - Tailor assessment to identify whether or not those controls are operating effectively
  - If you find nothing wrong, then you can assure them that control is in place
  - If it is broken, you will find out before the Wall Street Journal does….

How the CIO can answer the question…

Your work identifies weaknesses in the control environment that the CIO is accountable for designing and operating effectively, and gives them the opportunity to make improvements to those controls in a deliberate and planned manner, and support the statement :

"I am using an industry framework to evaluate and prioritize improvements to the control environment and am therefore fulfilling my role in IT governance"