IV. **Best Practices and Resources**

Best Practices:

Best Practices in the Information Assurance arena are complex, multivariate, international, regional, national, governmental and non-governmental, multi-sourced, range from the generic to the vendor specific, may require tailoring due to law or regulation, and require constant updating, training and education. It is the purpose of this chapter to present an overview of the key aspects of Best Practices, and to direct the reader to those sources of Best Practices most often identified in the literature as important sources regarding Information Assurance Best Practices.

Best Practices at a high level may be defined as:

> ***"Best Practices are those documented, accessible, effective, appropriate, and widely accepted strategies, plans, tactics, processes, methodologies, activities, and approaches developed by knowledgeable bodies and carried out by adequately trained personnel which are in compliance with existing laws and regulations and that have been shown over time through research, evaluation, and practice to be effective at providing reasonable assurance of desired outcomes, and which are continually reviewed and improved upon as circumstances dictate."***[1]

This definition of Best Practices suggests there are a minimum number of essential attributes that should be present for a body of work to be deemed Best Practices in Information Assurance such as:

Key Attributes of Best Practices in Information Assurance suggest they are:

a. Documented
b. Accessible
c. Tied to Standards promulgated by "Accepted Professional or Governmental" Bodies and are:
    i. Strategic
    ii. Tactical
    iii. Based on a Process and Methodology
    iv. Time and Practice Tested
    v. Provide assurance as to Defined Results
d. A Continual Process of Improvement, including continual Training, Education, and Certification)
e. Repeatable
f. Efficient - Benefits outweigh Costs

[1] University of Dallas Center of Information Assurance Best Practices definition. http://gsmweb.udallas.edu

g. Scalable - Pareto Analysis: The vital few and the trivial many
h. Effective - lead to desired outcomes
i. Adaptable and Address Contingencies
j. Provide Benchmarks and Frameworks,
k. In compliance with existing laws and regulations
l. Addressing the human, administrative, technical, and physical aspects: i.e.; people, processes, procedures, polices, plans, systems, networks, technologies, and facilities (P5STNF).

This top down definitional approach is helpful in understanding the essential fundamentals and Key Attributes of generic Best Practices and those elements pertinent to Information Assurance, but a further look at Best Practices Outcomes also identifies essential end points or results that any body of Best Practices should yield in Information Assurance implementations. They are:

Best Practices in Information Assurance have as Desired Outcomes the following:

a. **Availability** of information, systems, networks, devices, and personnel when needed,
b. **Authentication** of users and devices is made before access to resources is permitted,
c. **Integrity** of information, networks, systems, devices and personnel such that these elements are unimpaired and/or unaltered by unauthorized personnel,
d. **Confidentiality** of data is maintained and access to data is made to only authorized parties,
e. **Non-repudiation** that access to information or communication has taken place between network elements and/or authorized personnel and can be verified by an authorized third party, and
f. **Comply with all pertinent laws and regulations** such that Best Practices are continually updated relative to a changing legal and regulatory landscape.

While the Key Attributes and Desired Outcomes regarding Information Assurance Best Practices seem clear-cut, many issues remain. For instance:

a. Established Best Practices in Information Assurance may have to be modified because of the enactment of governmental regulations or laws: HIPAA, GLB,[2]
b. Multinational enterprises may have to operate under numerous sets of Best Practices because of varying legal requirements in

[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Gramm-Leach-Bliley Act, 1999 (GLB).

numerous jurisdictions: i.e., certain privacy legislation in Europe versus the United States may require different practices,[3]

c. The sheer number of promulgated Best Practices in Information Assurance by national, regional, and international governmental bodies, quasi-governmental bodies, professional organizations, universities, and vendors, makes it difficult to discern a single "Best Practices" model and hence, no single barometer against which due care and due diligence may be easily measured exists – see list of such organizations and Selected Best Practices following, and
d. The sheer number of professional certifications and certification bodies likewise makes it difficult to discern a single "Best Practices" certification in Information Assurance – see list of certifications and certification bodies following.

This situation of varying and complex "Best Practices" in Information Assurance is not unlike the myriad and complex set of homologation rules promulgated by many countries regarding telecommunications equipment that may be sold in those jurisdictions. Here, international telecommunications manufacturers wishing to have one, or only a few product designs that may be sold in many national jurisdictions with varying homologation rules, had to develop a complex array of the many (and sometimes conflicting) homologation requirements of each country they wished to sell product into. From this complex matrix, designs were then made to address those homologation rules relative to their most important markets.

> ***To date, in Information Assurance, there is no known array and/or mapping of the various, and sometimes disparate, Best Practices in a single codified Body of Knowledge. Hence, the practitioner is left to discern what Best Practices are pertinent to the facts and circumstances at hand.***

Recommended course of Action in discerning Best Practices in Information Assurance:

It is always prudent in dealing with complex issues to consult with knowledgeable industry professionals in order to arrive at a prudent course of action. This is particularly true when dealing in the complex area of Information Assurance Best Practices. However, in addition to seeking professional guidance, it is also pertinent to:

a. Insure the Best Practices being followed align themselves with the definition of Best Practices above.

[3] E.U. Data Protection Directive 95/46/EC approved by the Council and Parliament of the E.U. on October 24, 1995.

b. Insure the Best Practices being followed encompass the Key Attributes listed above,
c. Insure the Best Practices being followed adhere to the Desired Outcomes listed above, and
d. Insure the Best Practices being followed have been promulgated by an authoritative body in the Information Assurance arena.

These guidelines should assist the practitioner in finding one's way through the maze of complex constructs.

Resources:

Selected Best Practices Bodies of Knowledge

Institution	Best Practice	Web Site
International		
International Standards Organization (ISO)	ISO 15408 (Common Criteria) ISO 14516 IT Security Techniques ISO 17799 Code of Practice for Information Security Management	www.iso.org
International System Security Engineering Association	Systems Security Engineering Capability Maturity Model	http://www.sse-cmm.org now also ISO/IEC 21827
United Kingdom		
UK Dept. of Trade And Industry	BS 7799 Code of Practice for Information Security Management Code of Practice for Information Security Management	www.iso.org now codified as ISO 17799
Canada		
Canadian Security Establishment	Canadian Handbook on IT Security	http://www.cse.dnd.ca/en/about_cse.html
Germany		
Bubdesamt fur Sicherheit in der Informationstechunk	Baseline IT Protection Manual	in English at www.bsi.bund.de/gshb/English/menue.htm
Regional		
European Telecommunications Standards Institute	Baseline Security	www.etsi.org
National Standards Bodies of CEN countries	Security Categorization for Systems Protection of Healthcare Information ENV 12924 (1997	http://www.ncits
Organization for Economic Co-operation and Development	OECD Guidelines for the Security of Information Systems and Networks (and many other guidelines)	http://www.oecd.org/pdf/m0003000/m00033182.pdf
United States		
Center for Emergency Response (CERT)	The CERT Guide to System and Network Security Practices	published by Addison-Wesley
ISACA	CobiT Framework	www.isaca.org
National Institute of Standards and Technology	NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems Federal Information Processing Standards	www.nscl.nist.gov/nistpubs
U.S. Office of Management Budget	OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources	http.www.whitehouse.gov/WH/EOP//OMB/html/circulars/a130/a130.html
Purdue University	CERIAS Directory	http://www.cerias.purdue.edu/Infosec/hotlist/details.php?id-43

Selected Best Practices Bodies of Knowledge

Institution	Best Practice	Web Site
International System Security Engineering Association	Systems Security Engineering Capability Maturity Model	http://www.sse-cmm.org now also ISO/IEC 21827
National Security Agency	U.S. Common Criteria now ISO 15408	www.nsa.gov
	National Security Telecommunications Systems Security Instructions (NSTISSIs)	
	Security Guidelines Handbook	www.iscm.com/nsa.sec manual1.html
U.S. Department of Defense	U.S. DoD 8500.1 and 8500.2	www.dod.gov
The Internet Engineering Task Force (IETF)	Site Security Handbook RFC2196	www.ietf.org/rfc/rfc2196.txt?number=2196
Information Security Forum	The Forum's Standard of Good Practice: The Standard for Information Security	http://www.security forum.org
Software Engineering Institute Carnegie Mellon University	Numerous Documents	www.sei.cmu.edu/pub/documents
Federal Communications Commission	Network Reliability and Interoperability Council (NRIC) FCC Advisory Committee Best Practices	www.fcc.gov
Center for Internet Security MIT	Generally Accepted System Security Practices	http://web.mit.edu/security/www.gassp1.html
Center for Internet Security	Benchmarks 2002	www.cisecurity.org/bench.html
U.S. Technical Advisory Committee to ISO/IEC	NCITS / T4 – JTC 1 SC 27 IT(Information Technology Security Techniques (TR13335-1 through TR 13335-4	http://ncits.org/tc_home/t4htm/index.htm
Charles Cresson Wood CISSP, CISA	Information Security Policies Made Easy	www.baselinesoft.com PentaSafe Security Tech.
Tom Peltier	Information Security Polices, Procedures, and Standards: Guidelines for Effective Information Security Management	Auerbach, October 2001
Committee on Institutional Cooperation IT Security Working Group	Best IT Security Practices websites	http://www.itc.virginia.edu/policy/Policies/netdevices http://notes.utk.edu/Dll/Goodcit.nsf http://oit.utk.edu/aup/syslan.html http://www.itso.iu.edu/howto/bp http://net-services.ufl.edu/~security http://www.itpo.iu.edu http://itso.iu.edu/howto/bp/ http://www/itpo.iu.edu/Bestinfo.pdf

Selected Certifications:

Body	Certification	Web Site
SANS Institute	Global Information Assurance Certifications (GIAC) GIAC Security Essentials Certification GIAC Certified Firewall Analyst GIAC Certified Security Leadership GIAC Certified Intrusion Analyst GIAC Certified Incident Handler GIAC Certified Windows Security Administrator GIAC Certified Unix Systems Administrator GIAC Information Security Officer GIAC Systems and Network Auditor GIAC Certified Forensic Analyst GIAC IT Security Audit Essentials	www.sans.org
ISACA	CISA, CISM	www.isaca.org
ISC2	CISSP	www.isc2.org
NSA	IAM	www.nsa.gov
ACFE	CFE	www.cfenet.com
ASIS	CPP, PCI	www.asisonline.org
DRI Int'l.	ABCP, CBCP, MBCP	www.drii.org

GISA – Global Information Assurance Certifications – SANS Institute

ISACA - Certified Information System Auditor CISA, Certified Information Security Manager CISM certifications – Information Systems Audit and Control Association (ISACA)

ISC2 - Certified Information System Security Professional CISSP and System Security Certified Practitioner - SSCP certifications) see also International Information Security Certifications Consortium Code of Ethics. See also Information Systems Security Association – ISSA – www.issa.org.

IAM and CAE in IA - College and University Centers of Academic Excellence Accreditation in IA and other NSA certifications – Infosec Assessment Methodology – IAM certification, etc.

ACFE – Certified Fraud Examiners (CFE)

www.aicpa.org - WebTrust certifications

www.asisonline.org/cppg/cpphome.html - CPP Certified Protection Professional, PSP Physical Security Professional, PCI Professional Certified Investigator

Computer Security Institute (CSI) – www.gocsi.com

High Tech Crime Investigation Association – www.htcia.org

www.drii.org - DRI International – ABCP Associate Business Continuity Planner, CBCP Certified Business Continuity Planner, MBCP Master Business Continuity Planner

www.misti.org - MIS Training Institute – numerous courses on all aspects of IT and IT security including HIPAA.

www.cisco.com - see this site for vendor specific certifications
www.microsoft.com - see this site for vendor specific certifications