open.michigan

Author(s): Don M. Blumenthal, 2010

License: Unless otherwise noted, this material is made available under the terms of the **Attribution – Non-commercial – Share Alike 3.0 license** http://creativecommons.org/licenses/by-nc-sa/3.0/

We have reviewed this material in accordance with U.S. Copyright Law and have tried to maximize your ability to use, share, and adapt it. The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact **open.michigan@umich.edu** with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit http://open.umich.edu/education/about/terms-of-use.

Any **medical information** in this material is intended to inform and educate and is **not a tool for self-diagnosis** or a replacement for medical evaluation, advice, diagnosis or treatment by a healthcare professional. Please speak to your physician if you have questions about your medical condition.

Viewer discretion is advised: Some medical content is graphic and may not be suitable for all viewers.





Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

PD-GOV Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

PD-EXP Public Domain - Expired: Works that are no longer protected due to an expired copyright term.

PD-SELF Public Domain - Self Dedicated: Works that a copyright holder has dedicated to the public domain.

(cc) ZERO Creative Commons – Zero Waiver

(cc) BY Creative Commons – Attribution License

(cc) BY-SA Creative Commons – Attribution Share Alike License

(cc) BY-NC Creative Commons – Attribution Noncommercial License

(c) BY-NC-SA Creative Commons – Attribution Noncommercial Share Alike License

ONU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should do your own independent analysis to determine whether or not your use will be Fair.

Enterprise Security Program People and Processes

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues University of Michigan School of Information Week 12

More Alphabet Soup

- CRM Customer Relationship Management
- ERM Enterprise Risk Management
- ERP Enterprise Resource Planning
- SDLC Systems Development Life Cycle
 - Infosec Life Cycle Measure, improve, manage
- AAA Authentication, Authorization, Accounting

Loss Causes

- E-commerce boom.
 - Pressures to deploy.
- Attacks growth and complexity
- Immature security market
- Staff shortage
 - Expertise critical. Certifications secondary
- Mobile workforce and wireless
- Lack of unified approach
- Lack of ROI justification

Security Incentives

- Laws/regs
- Self-regulation
- Shareholders
- Customers
- Employees
- Business advantage
- Good citizenship?

People

- Strategy approach
- Components skills
- Administration management

Processes

- Strategy
- Components elements
- Administration

Cross Check

- Set long term goals for truly effective security program
- Audit

Evaluate

- Comprehensive ERM
- Overall governance programs and management commitment
- Overall business continuity and disaster recovery programs
- Identify core business initiatives on which most comprehensive IT check necessary
- Information security programs
- Compliance and ethics programs

More to Evaluate

- Records management systems and procedures
- IT understanding of business needs and efforts to factor them
- Process management
- Anti-fraud programs
- Quality of information used for decision-making