

**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](mailto: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. }



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



**Public Domain – Expired:** Works that are no longer protected due to an expired copyright term.



**Public Domain – Self Dedicated:** Works that a copyright holder has dedicated to the public domain.



**Creative Commons – Zero Waiver**



**Creative Commons – Attribution License**



**Creative Commons – Attribution Share Alike License**



**Creative Commons – Attribution Noncommercial License**



**Creative Commons – Attribution Noncommercial Share Alike License**



**GNU – 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.

# Real World Considerations

SI 510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues  
University of Michigan School of Information  
Week 10

# Assessment and Justification

- ▣ Risk assessment
- ▣ Role and purpose of risk assessment
- ▣ Return on investment
- ▣ Audit

# Information

- ▣ Risk – possibility that a threat is capable of exploiting a known weakness or vulnerability
- ▣ Risk assessment – operational process by which risks are identified and characterized
  - Explicit, repeatable process, which is well understood and followed continuously by all responsible parties

# Risk – An Overview

- ▣ Risk assessments help decision makers understand:
  - The things that could go wrong
  - How likely they are to occur
  - The consequences if they were to happen

# Knowing Where You Stand

- ▣ Understand the threats
- ▣ Identifying risks versus managing them
  - Risk assessments
    - ▣ Preventative measures
    - ▣ Reactive measures
  - Risk management
    - ▣ Maintains the effectiveness of measures once they have been put in place
    - ▣ Operational security

# Knowing Where You Stand

- ▣ Providing useful answers
  - What is the certainty of the risk?
  - What is the anticipated impact?
- ▣ Shaping the response
  - Probability of occurrence
  - Estimate of the consequences
- ▣ Priorities: matching resources against potential harm
  - Maximize operational deployment and resource use
  - Identifying risks with the greatest probability of occurrence, causing the greatest degree of harm



# Making Threats Visible

- ▣ Risk Classification
  - Risk identification
  - Risk estimation
    - ▣ Both entail assessment of risks to an entity
    - ▣ Both tend to be more qualitative than quantitative
    - ▣ Both result in plausible evidence to support decision making about the response

# Risk Identification

- ▣ A range-finding activity
  - Simplest form of risk classification
  - Identify potentially harmful risks
    - ▣ Gap analysis
  - Document characteristics of every vulnerability
    - ▣ Itemize a list of threats that would be able to exploit it
  - Track latent threats that could exploit a known vulnerability

# Risk Estimation

- ▣ A data-driven process
  - Measure and quantitatively describe each potential risk
    - ▣ Assets affected
    - ▣ Potential duration of the threat
    - ▣ Severity of adverse impact
  - Provides substantive data that will serve as the basis for the risk analysis
  - Determines the probability and impact of identified threats
  - Provides data for the analysis and decision making

# Return on Investment

- ▣ *Security metrics are the servants of risk management, and risk management is about making decisions. Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk.*
  - *Daniel E. Geer, Jr., SC.D.*

# ROI Strategy Formulation

- ▣ ROI
  - Identify the adverse impact of threat in terms of cost
  - Ensure that the countermeasure does not cost more than the harm that the threat could cause
- ▣ Trade-offs
  - Likelihood of occurrence
  - Frequency of occurrence
  - Unit cost for each occurrence

# Making ROI Decisions

- ▣ Basic concept
  - Annualized Loss Exposure (ALE) = Annual Cost of Deployment – (Annual Rate of Occurrence × Cost per Occurrence)
- ▣ Certainty factors – assuring credibility
  - Express degree of certainty of the estimate as a level of confidence from 0 to 100 percent

# Security Solution

- ▣ Analyze risk
  - Task – understand precisely the implications of the threat picture
  - Goal – refine further to a point that can be acted on by decision makers
  - Specify a minimum degree of protection to assess the risk-tolerance
- ▣ Assign priorities
  - Understanding the cost/benefit situation
  - Making a risk-mitigation decision
    - To reduce the severity or effect of a known risk
    - To ensure recovery through a risk transfer

# Security Solution (2)

- ▣ Ensure confidence
  - The value of a standard method
    - ▣ Organization will have data to support decisions about which item to secure and in what order
    - ▣ Organization will be able to increase its predictive accuracy and thus sharpen its security control
- ▣ Document outcomes
  - Risk mitigation report specifies:
    - ▣ Steps selected for each risk
    - ▣ Countermeasures that will be implemented
    - ▣ Parties responsible for accomplishing each task



# Plan

- ▣ Establish a standard schedule for the performance of each assessment
- ▣ Define a process for problem reporting and corrective action
- ▣ Plans for risk assessment should ensure that each assessment produces consistent data
  - Interprets the degree of risk exposure, as well as the types of countermeasures that have to be deployed
  - Provides an understanding of the precise nature of the threats and the required response

# Do

- ▣ Implement the operational risk assessment process
  - Ensures that adequate resources are available to support the assessment activities
  - Plan should specify the means or criteria that will be used to determine whether the goals of the process are met

# Check

- ▣ Judge performance – importance of standard criteria
  - Allows to judge with certainty, at any time, for any countermeasure, whether:
    - ▣ That control is performing as desired
    - ▣ It continues to achieve its purpose
  - The data is used to monitor and ensure the effectiveness of its information assurance scheme

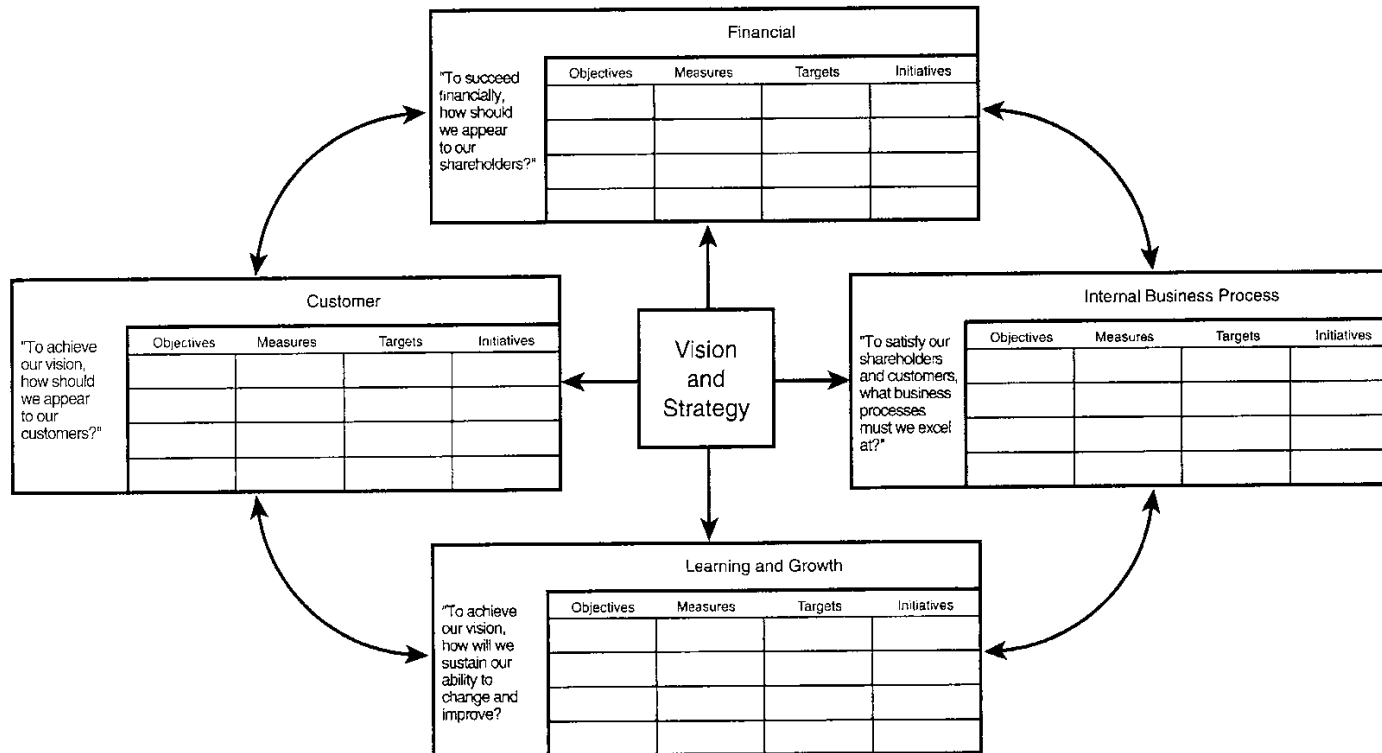
# Balanced Scorecard List - 1

- ▣ Financial Perspective Measures
  - Net Income
  - Operating Margin
  - Economic Value Added
  - Revenue Growth
  
- ▣ Operational Perspective Measures
  - Safety
  - Process Enhancement
  - Operational Efficiency
  - Productivity

# Balanced Scorecard List - 2

- ▣ Customer Perspective Measures
  - Customer Satisfaction, external
  - Customer Satisfaction, internal
  - Customer Loyalty
- ▣ Learn Grow Perspective Measures
  - Employee Personal Development
  - Employee Satisfaction
  - Organizational Enhancement

# Balanced Scorecard Process



**Figure 8-1** The Balanced Scorecard (Redrawn)

Reprinted by permission of *Harvard Business Review*. Exhibit from "Using the Balanced Scorecard as a Strategic Management System" by R. Kaplan and D. Norton, January–February 2006, p. 75. Copyright © 1996 by the Harvard Business School Publishing Corporation; all rights reserved.

# Audit

- ▣ “Assures the integrity of the security solution from the pervasive influence of process entropy”
- ▣ Aims of an audit
  - Identify non-compliance with particular, specified audit criteria
  - Certification: the basis for the audit is a general standard, or model that is typically specified by a third party

# Kinds of Audits

- ▣ Internal/external
- ▣ Security – to verify compliance with specified requirement
- ▣ Follow-up – previous audit requires follow-up
- ▣ Contractual – to determine whether system meets a customer's contractual requirements



# Information Assurance Audits

- ▣ Information assurance audits
  - Completeness and correctness of the policies that guide the process
  - Execution of the procedures to carry out the process
  - Capability of the management