

Did you know?

GRAMM-LEACH-BLILEY ACT

A risk management process is required to protect student financial information:

Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information ...

Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

HIPAA SECURITY RULE

A risk management process is required to protect health data:

Risk analysis (Required [by law]). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Risk management (Required [by law]). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).



Information Security & Privacy
Information Technology Services
Phone (419) 372-0999


infosec@bgsu.edu
<http://www.bgsu.edu/infosec>

B06-0002-01



ADVANCED INFORMATION STEWARDSHIP

MANAGING RISK

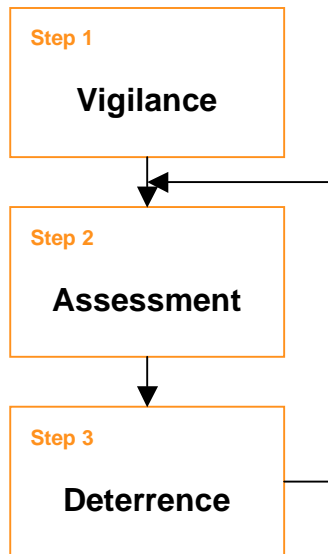


GETTING STARTED

Information Security & Privacy
Advice

(ISO/IEC 17799:2005 § 6.1.2.f)

BASIC CONCEPTS



The approach is **easy** and **natural**.

- ① You pay attention to relevant factors in your environment.
- ① You assess the impact.
- ① You mitigate the risks, evaluate results, make adjustments, and repeat the process.

EXAMPLE

You are on the turnpike. **[Vigilance]** The gas gauge shows $\frac{1}{4}$ tank. **[Assessment]** Where is next rest stop? How far can I go? **[Deterrence]** Stop and fill up. Periodically monitor.

STEP 1 - VIGILANCE

Applying this simple risk management approach to information security, first check your “gauges” - gather information from the following:

- ① BGSU Mission, policies, and State or Federal regulations.
- ① Organization plans & capabilities.
- ① Customer & competitor trends.
- ① Technology changes & trends.
- ① Industry news, consultant reports.
- ① Security vulnerabilities & threats.
- ① Security best practices.

For assistance, see:

<http://www.bgsu.edu/infosec>

(Follow Advice links to Risk Management advice for faculty and staff to the navigation map.)

STEP 2 - ASSESSMENT

How far can I reasonably go? What is my capacity? What happens if I run out of “gas”? Evaluate:

- ⚠ *Internal Strengths*
- ⚠ *Internal Weaknesses*
- ⚠ *External Opportunities*
- ⚠ *External Threats*

An ethical risk assessment adhering to BGSU core values should be performed from multiple perspectives: Organization, team, and each individual.

STEP 3 - DETERRENCE

Using the information developed in Step 2:

- ⚠ *Develop* a realistic plan comprised of goals & controls
- ⚠ *Implement* policies & procedures. Train staff.
- ⚠ *Evaluate*, test, or audit results.

REPEAT THE PROCESS

Make adjustments or improvements as necessary, including more robust or quantitative risk analysis. Supply feedback for continuous improvement.

EXAMPLE

You have a deadline and desire to copy sensitive information to a USB memory drive and take it home to work on it.

[Vigilance] News reports reveal that many home systems are not secure or media was easily lost, and companies had to inform customers of breaches. **[Assessment]** Your system *has* been acting strange lately. Maybe it has a virus. The USB drive is small and *would be* easy to lose...

[Deterrence] You instead obtain permission to take work home on a University-secured laptop with an encrypted hard drive. You then update area policies and advise co-workers.

www.bgsu.edu/infosec