INFORMATION SECURITY

BKD LLP
CPAs & Advisors

experience **insight** // Identity theft, network hacking and natural disasters could occur at any time and expose your company's vital information. How confident are you that your information systems are secure? The compliance environment created by Sarbanes-Oxley (SOX) legislation, the *Gramm-Leach-Bliley Act* (GLBA), *Health Insurance Portability and Accountability Act of 1996* (HIPAA) and other regulations requires you to take specific measures. BKD's information security professionals can help identify and manage your risk with best practices and knowledge of industry-specific regulations.

RISK **ASSESSMENT**

A risk assessment is the foundation of an information security program. Without a secure profile, you risk giving electronic intruders the keys and codes to your company.

A risk assessment identifies possible risks to the security of an organization's information systems. Our process is based on guidelines from the National Institute of Standards and Technology's (NIST) Risk Management Guide for Information Technology Systems and involves:

- Analysis of critical assets, security requirements and potential threats
- Evaluation of infrastructure vulnerabilities
- Report and recommendations for protection strategy

PENETRATION **TESTING**

To help identify network vulnerabilities and weaknesses, we apply tools and techniques used by hackers, identity thieves and disgruntled employees to analyze and attempt to exploit any security issues. Depending on your needs and the depth of testing desired, we perform the following:

NETWORK SCANNING // Port scanners determine existing devices, open ports and services operating on these ports—a beginning step for full penetration testing.

VULNERABILITY SCANNING // This identifies network hosts, services, operating system, applications and related vulnerabilities—a highly automated scan based on a database of vulnerabilities.

PENETRATION TESTING // Network and vulnerability scanning is combined with the human element—a process that emulates a true hacking approach. External penetration testing simulates Internet-based attacks. Internal penetration testing simulates attacks by individuals who have breached your network's perimeter defenses.

IT **REVIEW**

An IT review evaluates the controls within your company's IT infrastructure. Our review evaluates your information system's ability to safeguard assets, maintain data integrity and operate effectively to achieve your objectives. Our tested methodologies and services address current regulatory environments, such as Federal Financial Institutions Examination Council (FFIEC), HIPAA, GLBA and SOX.

An IT review can help identify risks in areas such as:

- Identity theft
- Physical security
- Logical security
- Business continuity planning
- Information security
- Vendor management
- Internet security

2250 **CPAS, ADVISORS & STAFF**

Work face to face with one of approximately 2,250 CPAs, advisors and dedicated staff, and **experience round-the-clock commitment** to ideas that help improve performance.

> “As part of our ongoing risk assessments, we utilize BKD’s expertise to improve our internal controls. BKD’s penetration testing and assessments provide a new perspective and enhanced confidence in the safeguards we have in place to protect our customers’ information. Its IT review recommendations are based on practical experience gained from other financial institutions, which benefits us with improved policies and procedures. We have a shorter learning curve with BKD and confidence in its recommendations.”

Alan L. Fosler

Senior Vice President & Cashier *Union Bank and Trust Company*

SOCIAL **ENGINEERING**

Often referred to as the single greatest security risk, social engineering is the practice of obtaining confidential information for user manipulation.

Our process includes attempts to circumvent current security controls by gaining information from employees and/or vendors. This includes simulated pretext phone calling, spoofing, phishing, physical access attempts and the use of malware and counterfeit websites for security testing. It is followed by an evaluation of the organization’s security posture, test of the incident response plan and efforts to raise employee awareness.

BUSINESS CONTINUITY **PLANNING (BPC)**

Advance preparation for a security crisis or disaster could mean the difference between the survival and demise of a business. We work with organizations to develop a plan for the maintenance or recovery of business operations should an adverse event occur. Our services include:

- BCP program setup and management
- Business impact analysis and risk assessment
- Plan and policy development
- Program assessment, validation and verification

ABOUT BKD **IT RISK SERVICES**

BKD IT Risk Services, a division of **BKD, LLP**, a national CPA and advisory firms, combines the resources of experienced, certified corporate governance and information security professionals dedicated to the risk management industry.

1:5 **PARTNER:STAFF**

With a partner-to-staff ratio much lower than the 1-to-9 average found in other top firms, you’ll have access to partners and **experience personal communication.**

BKD THOUGHTWARE™ // articles // emails // presentations // videos // webinars

bkd.com

FOR MORE INFORMATION // For a complete list of our offices and subsidiaries, visit **bkd.com** or contact:

BKD LLP **CPAs & Advisors**

Cindy Boyle // Partner

cboyle@bkd.com // 501.372.1040