September 03, 2015

RESPONSE TO REQUEST FOR INFORMATION (RFI)

Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring,and Restoration Services

Confidential & Proprietary

Prepared for:

Florida Department of Management Services

Joel Atkinson
4050 Esplanade Way
Suite 360
Tallahassee, Florida 32399-0950

Submitted by:

Integrated Computer Solutions, Inc.

Shandy Strivelli
60 Commerce Street, Suite 1100
Montgomery, AL 36104
shandy.strivelli@icsinc.com

INTRODUCTION

Founded in 1997, Integrated Computer Solutions, Inc. (ICS) is a privately-held, full-service information technology (IT) and security consulting firm incorporated in the State of Alabama, with headquarters in Montgomery, Alabama. ICS is an "S" type corporation, and our FEIN is 1361825. ICS is licensed to do business in the states of North Carolina, Alabama, Florida, California, Delaware, Mississippi, Georgia, Idaho, Pennsylvania, Texas, Utah, and Virginia. In addition to our headquarters in Montgomery, Alabama, ICS also maintains an office in Tallahassee, Florida.

Over the past 18 years, ICS has had the good fortune to serve numerous agencies throughout the State of Florida and many other state agencies with premier Cyber Security and Risk Assessment Services that range from:

- Incident Response and Forensics support
- Business Continuity Planning (BCP) and Continuity of Operations Planning (COOP)
- Disaster Recovering Planning (DRP)
- Enterprise Risk Assessments
- Technical Security Assessment including vulnerability assessment, penetration tests, web application assessments, phishing, ethical hacking, etc.
- Project Management and Staff Augmentation

ICS maintains an office and team of certified professionals in Tallahassee who are ready to support the needs of the state agencies both locally and by leveraging the expertise and experience of the entire Integrated Computer Solutions, Inc. team around the United States.

Below is a sampling of the many engagements across Florida and southeastern state governmental agencies.

Security Risk Assessment

- Florida Department of Highway Safety and Motor Vehicles (2010, 2012, 2015)
- Florida Agency for Health Care Administration (2011, 2013)
- Florida Department of Family and Children (2013)
- Florida Department of Transportation (2011, 2013, 2015)
- Florida Agency for Workforce Innovation / Florida Department of Economic Opportunity (2009 - 2011)
- Florida Department of Financial Services (2011 - 2012)
- Florida Department of Law Enforcement (2011)
- Mississippi State Department of Health (2009-2014)
- Mississippi Department of Employment Security (2011-2012)
- Mississippi Department of Education (2011)
- Mississippi Department of Corrections (2011)
- Mississippi Department of Architecture (2011)

- Mississippi Board of Massage Therapy (2011)
- Mississippi Board of Licensure for Professional Engineers and Surveyors (2014)
- North Carolina Department of Public Safety (2013)
- North Carolina Department of Health and Human Services (2014)
- North Carolina Department of Revenue (2014)
- Tallahassee Community College (2012)
- Unified Port of San Diego (2013-2014)
- Valencia College (2014 - 2015)
- Auburn Montgomery (2010, 2015)
- Duval County Public Schools (2009, 2012, 2014)
- Alabama Information Services Division (2009 - Present)
- Alabama Department of Conservation and Natural Resources (2013-Present)
- Alabama Medicaid Agency (2012 - Present)
- Alabama Supreme Court (2015)
- Miami Dade State Attorney's Office (2014)

Disaster Recovery Planning and Implementation

- Navigate Affordable Housing Partners (7/2010 - Present)
- Duval County Public Schools (2009, 2012, 2013)
- State of Mississippi - Department of Health (7/2011 - 12/2014)
- State of AL - Department of Industrial Relations (4/2006 - 3/2007)
- Montgomery Water Works (4/2007 - 9/2011)
- Riverside County, CA (8/2006 - 3/2008)

Continuity of Government Initiatives

- State of FL - Agency for Health Care Administration (6/2006 - 12/2013)
- State AL - Treasury (3/2008 - 5/2009)
- State of FL - Dept of State - Division of Elections (7/2006 - 6/2007)
- Montgomery Water Works (4/2007 - 9/2011)

Web Application Security Assessment

- Alabama Department of Revenue (2012 - Present)
- Alabama Medicaid Agency (2012 - Present)
- Duval County Schools (2009)
- Alabama Supercomputer Authority(12/2008 - present)
- State of FL - Agency for Workforce Innovation (8/2007)
- Atlametrics (9/2009 - 12/2009)

- St. Johns County Schools (June 2009 - current)

Penetration Testing

- Florida Department of Highway Safety and Motor Vehicles (2010, 2012, 2015)
- Florida Agency for Health Care Administration (2011, 2013)
- Florida Department of Family and Children (2013)
- Florida Department of Transportation (2011, 2013, 2015)
- Florida Agency for Workforce Innovation / Florida Department of Economic Opportunity (2009 - 2011)
- Florida Department of Financial Services (2011 - 2012)
- Florida Department of Law Enforcement (2011)
- Mississippi State Department of Health (2009-2014)
- Mississippi Board of Licensure for Professional Engineers and Surveyors (2014)
- North Carolina Department of Public Safety (2013)
- North Carolina Department of Health and Human Services (2014)
- North Carolina Department of Revenue (2014)
- Tallahassee Community College (2012)
- Unified Port of San Diego (2013-2014)
- Valencia College (2014 - 2015)
- Auburn Montgomery (2010, 2015)
- Duval County Public Schools (2009, 2012, 2014)
- Alabama Information Services Division (2009 - Present)
- Alabama Department of Conservation and Natural Resources (2013-Present)
- Alabama Medicaid Agency (2012 - Present)
- Alabama Supreme Court (2015)
- Miami Dade State Attorney's Office (2014)
- Alabama Department of Revenue (2012 - Present)
- Florida Agency for Health Care Administration (6/2006 - 12/2014)
- Duval County Schools (2009, 2012)
- Florida College Center for Library Automation (2008, 2010, 2011)
- Montgomery Water Works (4/2007 - 9/2011)
- DeKalb County Regional Health System (6/2010 - 7/2010)
- St. Johns County Schools (June 2009 - current)
- Tallahassee Community College (2/2008 - 6/2008)
- Alabama Supreme Court (2015)
- Miami Dade State Attorney's Office (2014)

- Alabama Department of Revenue (2012 - Present)
- Florida Agency for Health Care Administration (6/2006 - 12/2014)
- Duval County Schools (2009, 2012)
- Florida College Center for Library Automation (2008, 2010, 2011)
- Montgomery Water Works (4/2007 - 9/2011)
- DeKalb County Regional Health System (6/2010 - 7/2010)
- St. Johns County Schools (June 2009 - current)
- Tallahassee Community College (2/2008 - 6/2008)
- ThyssenKrupp Steel (10/2009 - 11/2009)

Network architecture assessment

- State of AL, ISD (7/2004 to present)
- Montgomery Area Chamber of Commerce (10/2005 - present)
- BELCO Credit Union (2007 - 12/2008)
- Hillsborough County Airport Authority (12/2007-4/2008)
- Lee County Port Authority (5/2008 - 8/2008)

Digital Forensic Support

- State of AL - ISD (7/2004 to present)
- State of AL - Insurance Department (2/2004 - 4/2004)
- Southern Poverty Law Center (2/2006 / present)
- Fowler White (Oct 2006 - Mar 2007)
- S142-09A (Aug 2009)
- C168-08A (8/2008 - 10/2008)
- S116-07A (2/2008 - 1/2009)
- C031-08A (2/2007)

Note: Due to the highly confidential nature of forensics engagements, ICS is legally obligated to refrain from disclosing the names of some of our clients. In lieu of providing customer names, ICS has provided client account numbers.

ICS is uniquely qualified to meet the needs of the State of Florida, for the following reasons:

1.) **Qualifications:** Nearly 18 years of Cyber Security Experience supporting US Department of Defense, State Agencies, and Commercial Organizations throughout the United States.
2.) **Experience:** ICS's team of highly qualified trained and certified professionals possess the most up-to-date skills and expertise to meet the needs of the Department.
3.) **Past Performance:** As our satisfied customers will tell you, ICS utilizes its proprietary project management methodology to ensure our team understands our customers' requirements so that we can anticipate, meet and exceed their requirements each and every time.

BACKGROUND

In performing a comprehensive Cyber-Security Response Assessments, whether security program or single application level, ICS will gain an understanding of each agency's security organization and environment including perspectives from management, operations, and technical subject matter experts.

ICS will analyze the program itself as well as the architecture in place and determine the efficacy and adequacy of the program standards, the associated resources while also determining where any gaps may exist between policies and actual practice.

Reviews are completed at the organizational, mission/business process, and information systems tiers using a structured approach to ensure we capture strengths and weaknesses in governance, information & information flows and the operational environment.

Finally, ICS will provide a series of reports from executive summaries to detailed technical reports, each written to the appropriate audience, to support risk based decision support at the business level and the remediation of any vulnerabilities. Where appropriate, ICS provides customers a prioritized list of remediation activities along with their associated costs. Focus is always on leveraging existing security controls to minimize cost before considering additional security expenditures.

ICS is able to provide most of the pre-incident and post-incident services requested. In effort to aid in reviewing our response, we have responded to the key sections identified in the RFI by referencing the RFI section(s) where appropriate. Each header identifies the relevant section of the solicitation addressed by our response.

CONTACT INFORMATION

Integrated Computer Solutions, Inc. (ICS)

Keith Young,

CISSP, CCFE, CHFI

Executive Practice Manager

Over 15 years as an information technology and security professional leading a team of consultants to solve organizational, technical, and people-related challenges. Experienced consultant, IT manager, security engineer, researcher, and instructor working with state/local governments, utilities, retail organizations, and financial services institutions. Lead consulting practice areas: Technical Security, Risk Assessments, Staff Support, Incident Response/Forensics, Disaster Recovery and Business Continuity Planning.

Office: 334.356.4512
Email: Keith.Young@icsinc.com

1(A) INCIDENT RESPONSE AGREEMENTS

Overview

ICS will guide each agency through the process of creating agreements that will reduce liability and clarify the necessary terms and conditions required to ensure the quickest and most effective response to a cyber-security incident. ICS' approach to composing pre-incident response agreements includes the following:

Gathering Historical Information

ICS recognizes the value of lessons-learned from past incident response, and will survey each agency's Subject Matter Experts (SMEs) on deficiencies discovered in historical agreements. ICS will also collect and conduct a thorough review of a sample of agreements provided by SMEs. Results from SME surveys and document review will help ICS create a customized list of known agreement-related pitfalls to be avoided for each agency.

Analyzing Current Trends and Best Practices

ICS will search open source intelligence on the current threat trends relevant to the implementation of technology, industry and governance model similar to each agency. This research will help ICS to customize agreement language to better fit each agency's anticipated agreement needs.

Ensuring Multi-Requirement and Multi-Partner Coverage

Many agencies must comply with more than one legal mandate and several regulations. They may also share data with external partners. For example, requirements for what constitutes an incident, expected response times and retention of data related to the incident, varies. They may vary from regulation to regulation or from agency to agency. ICS will guide agencies through creating agreements covering multiple, and sometimes, competing requirements. These agreements will satisfy internal and external expectations. That comprehensive matrix will then be applied to final agreement language.

1(B) ASSESSMENTS

Overview

ICS will evaluate each agency's current state of information security and cyber-security incident response capability, by taking many things into consideration, including but not limited to:

- Adequacy of policies, emergency management and incident response plans
- Ability to collect and use intelligence to make informed risk decisions
- Sufficiency of communications with internal and external partners
- Effectiveness of controls to detect, prevent or respond to security events
- Investigative and forensic capabilities
- Mitigation and recovery controls
- Staff awareness and training levels
- Ability to track losses and costs
- Level of understanding of mandated requirements related to incident response, investigations and reporting
- Our assessment process is divided into pre-assessment, assessment, and post-assessment phases.

The pre-incident assessment effort will include the following three phases and risk rating:

Pre-Assessment Phase - Customize the Threat Landscape

ICS begins assessments by searching open source intelligence on the current threat trends relevant to the implementation of technology and governance structure similar to each agency, (e.g., the same network devices, operating systems, databases, applications in physical, virtual and cloud infrastructures and regulations). This research helps ICS to customize the assessment tools used for the engagement to better fit each agency's threat profile.

Assessment Phase - Gather Information

ICS learns more about each agency, through conversation with Subject Matter Experts (SMEs). We also rely heavily on any documentation collected from SMEs to identify gaps in cyber-security incident specific plans, training, policies and procedures. All relevant controls are then evaluated for existence and effectiveness.

Post Assessment Phase - Aggregate and Analyze Information

Once the interviews are conducted and documentation is reviewed, ICS compiles the information extracted from all sources. Then we convert the raw vulnerabilities into risks, based on the following methodology:

- Categorizing vulnerabilities (e.g., incident response process flaws vs. inadequate enforcement);
- Pairing with threat vectors (e.g., data breach vs. damage to server); and
- Assessing the probability of occurrence and possible impact.

1(B) ASSESSMENTS CONTINUED

Risk Rating

The findings will be distilled into a few key issues and rated as high, medium, or low to help leadership prioritize which risks require more immediate attention:

- A priority of **High** identifies either an immediate or serious threat; or actions that should provide significant benefits to the security program if implemented;
- A priority of **Medium** represent a threat that is not immediate or seriously damaging in nature; or actions that should provide moderate benefits to the security program; and
- A priority of **Low** represent threats that are either minor in scope or not immediate in nature; or actions that should provide minor, but worthwhile, benefits to the security program.

1(C) PREPARATION

Overview

Having served as a trusted adviser to many agencies in various jurisdictions and numerous industries, ICS understands that a *one-size-fits-all* approach to cyber-security incident response preparation leads to reduced effectiveness and higher costs. ICS will provide guidance on requirements and best practices that matches each agency's unique threat profile. We will cover the following when providing pre-incident preparation services:

Categorization

A cyber-security incident could entail almost anything. Responders may be dealing with one isolated instance of a policy violation; or they could be faced with a large-scale, unauthorized extraction of confidential information. Because the range is so wide and the stakes are so high, ICS will guide each agency through finding those high level set of concepts and descriptions that enable improved communications among and between agencies. The resulting taxonomy will not replace discipline (technical, operational, intelligence) that needs to occur to defend agency computers/networks, but provide a common platform to execute their mission. Each agency will be able to utilize the incident and event categories and reporting time-frames to ensure optimal effectiveness.

Ensuring the categorization of incidents helps responders to promptly implement the correct and targeted response to any cyber-security incident, is **not the only goal**. ICS will also roll-up categorization efforts from individual agencies to the State level, and coordinate with Florida's **Agency for State Technology** to ensure categorization taxonomies facilitate state-level objectives for cyber-security incident tracking, trending and reporting.

Risk Management

Compliance requirements help to establish a good cyber-security baseline to mitigate known risks, but do not adequately address cyber threats that continuously change with increasing intensity and complexity, or protect against sophisticated adversaries. ICS will not only guide each agency through implementing a checklist of requirements; but also creating a plan for managing cyber risks to an acceptable level. Managing cyber-security risk as part of an agency's governance, risk management, and business continuity frameworks provides the strategic framework for managing cyber-security risk throughout each enterprise. Some example of questions each agency will answer to create their risk management plan include:

- How are we informed about the current level and business impact of cyber risks to our agency?
- What is the current level and business impact of cyber risks to our agency? What is our plan to address identified risks?
- How does our cyber-security program apply industry standards and best practices?
- How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
- How comprehensive is our cyber incident response plan? How often is it tested?
- How can we shift from being less reactive to more proactive?

1(C) PREPARATION CONTINUED

Requirements vs. Best Practices

Agencies will encounter major challenges when responding to cyber-security incidents if they lack clearly defined requirements. To help agencies avoid these challenges, ICS will review each agency's requirements management process to ensure they are taking a truly systematic approach to finding, documenting, organizing and tracking requirements and any changes that may occur. Where deficiencies are discovered, ICS will recommend mitigation strategies.

However, ensuring compliance with cyber-security incident response requirements is not enough. To truly optimize risk management, agencies should also leverage best practices that have been proven to reduce the costs of a security breaches and heighten the security expertise of responders. ICS will include best practice guidance from many reliable sources, including, but not limited to:

- Federal - Some examples include the National Institute of Standards and Technology (NIST), the Federal Emergency Management (FEMA) and the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT)
- Regulations - The the Health Insurance Portability and Accountability Act (HIPAA), the Criminal Justice Information System (CJIS) Security Policy, and The Payment Card Industry Data Security Standard (PCI DSS)
- Standards - Multiple standards from the International Organization for Standardization (ISO) such as ISO/IEC 27035 Security incident management, and the Capability Maturity Model Integration (CMMI) for Services.
- Proprietary - Some of the best guidance comes from the vendors or industry partners supplying the software, hardware and firmware tools needed to handle cyber-security incidents.

1(D) DEVELOPING CYBER-SECURITY INCIDENT RESPONSE PLANS

Overview

Cyber-Security incident response may vary, based on the nature and severity of the incident. However, the life-cycle of an incident doesn't usually change. ICS will ensure that each agency is guided through creating a cyber-security plan to deal with all incidents in a consistent manner. Assisting in the development of written State Agency plans for incident response will, at a minimum, include guidance on the following phases of an incident lifecycle:

Preparation

ICS will help agencies to identify deficiencies in their existing incident preparation processes. Preparation is key and entails staff being well trained on identifying:

- The start of an incident
- When and when not to respond to an incident
- How to respond
- Who should respond
- How to recover
- Creating established security policies, procedures and plans
- Communication do's and don'ts

Other aspects that ICS will assist agencies with is evaluating the sufficiency of training and pre-deployed incident handling assets. When training for an incident agencies should contemplate different types of training for team needs such as software support, specialized investigative techniques, incident response tool usage, and environmental procedure requirements. When looking at pre-deployed incident handling assets, certain tools must be in place in case of a system breach. This includes monitoring of sensors, probes, and monitors on critical systems, tracking databases in core systems and completing active audit logs for all server network aspects and components.

Identification

ICS will assist agencies in properly identifying an incident so that, not only will the correct response be taken promptly, but that incident closure will ensure appropriate reporting to internal and external partners occurs, and trending information is gathered to avoid future incidents of similar nature.

Containment

Understanding the difference between protecting evidence from an incident and containing an incident to prevent further impact is critical. If evidence is destroyed, it may be difficult to determine the root cause or conduct other activities, such as prosecution when necessary. ICS will assist agencies in creating containment strategies based on the type of incident. Criteria for determining the appropriate strategy may include:

- Potential damage to and theft of resources
- Need for evidence preservation

- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

Eradication

ICS will ensure agency plans incorporate guidance on what to do after an incident has been contained and evidence has been preserved, as appropriate, eradication is necessary to eliminate components of the incident. Deleting malicious code and disabling breached user accounts are examples of eradication.

Recovery

During recovery, IT Administrators restore systems to normal operation and, as necessary, harden systems to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and adding or strengthening other security controls. ICS will guide agencies on how to incorporate recovery activities in their plans.

Recovery also has a proactive side, which results in designing services and systems that ensure recovery is faster and easier. So ICS will ensure that plans include ties to Problem Management and Service Design processes, when applicable.

Follow-up

ICS will guide agencies through creating plans that ensure incident closure includes proper closure activities. Incident closure should give agencies ample time to ensure the repaired service is really working, but it should not be so far into the future that users and staff have difficulty reconstructing what the parameters of the actual failure were.

1(E)TRAINING

Overview

Incident response training should cover more than a random set of IT security topics or align with compliance requirement objectives. Training should be comprehensive and strategic. Training should ensure that staff with varying roles are equipped to promptly and effectively respond to the diverse cyber-security events most likely to occur. ICS can assist agencies in creating those strategic and comprehensive training targets and, if necessary, ICS can deliver the training to staff as well. ICS' guidance and review of training policies, procedures and content will address the following for each agency:

Policy and Procedure

ICS will assist agencies with creating a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. We can also evaluate procedures to ensure they facilitate the implementation of the security awareness and training policy and associated security awareness and training controls and instruction on how to keep the policy and procedures current and relevant.

Training Content

ICS will guide agencies on composing new or evaluating existing training. ICS will recommend different content types (e.g., content for new users vs. veterans or content for breaches impacting confidentiality vs malware events) and different content presentations (e.g., online, simulation drills, documents, and table-top exercises) that best meet their needs.

Role-Based

ICS will help agencies determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of agencies and the information systems to which personnel have authorized access. Agencies must provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Evaluations of training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs will also be evaluated. Role-based security training also applies to contractors providing services to State agencies.

2(B) INVESTIGATION AND CLEAN-UP

Overview

ICS has extensive experience conducting discreet and rapid evaluation of incidents, leading investigations and providing remediation services to restore operations to pre-incident levels.

Objectives of Investigation and Cleanup

ICS understands that incidents involving stored, transmitted, or processed data require different investigative and cleanup methods than those involving safety of personal or damage to resources. Additionally, investigations should be conducted in a flexible stepped approach whereby the results of preceding steps are used as rationale and justification for subsequent steps. With State staff approval, steps may be modified, combined or conducted concurrently at different locations on one facility to best suit the needs of a particular site. All work must be conducted in a safe manner and in accordance with all appropriate local, state, and federal rules and regulations.

ICS will help agencies to determine the appropriate investigative and cleanup approaches and the level of concern necessary to correctly mitigate risks and reduce damages. Some objectives of investigative guidance will include the determination of:

- Likely sources of the contamination or breach
- Extent and magnitude of contamination or breach (e.g., impact to safety, confidentiality, privacy, availability or integrity)
- Actual or potential impacts relating to the incident
- Information needed for designing any necessary corrective actions
- Information needed for appropriate notifications to affected parties

ICS will also guide agencies through creating a work plan for cleanup that ensures remediation is monitored until it is permanent.

2(C) INCIDENT RESPONSE

Overview

ICS is uniquely qualified to provide guidance to assist State Agencies in response to an incident, having acted as an adviser to organizations across many jurisdictions, sizes, capabilities and bound to many requirements and standards for over 18 years.

Quick, Discreet and Experienced

Records of cyber-attacks have almost doubled since last year, suggesting that the need to investigate an incident is imminent for all agencies. ICS Incident Response Services will provide the experience and discreet technical expertise to accelerate incident investigation and containment. Our teams can work together with in-house teams and external partners for all stages of incident response from analysis and detection through containment, remediation and cleanup.

ICS incident response teams are made up of industry-leading experts with decades of combined experience in incident response of all sizes. ICS will help agencies with all aspects of the response from identification through incident remediation and clean-up. Confusion will be avoided by ICS providing a single point of contact who is ultimately responsible for coordinating, communicating, and reporting on all aspects of incident response activities. Incident management includes all aspects of threat detection, documenting findings and collaborating to devise appropriate remediation activities. Experienced incident responders with forensic backgrounds are prepared to respond to compromises of all sizes and severity. ICS will guide agency staff through rapid analysis and incident scoping.

2(D) MITIGATION PLANS

Overview

The impacts of a cyber intrusion will be different for every incident depending on the nature of the compromise and existing capabilities to respond. Each agency must assess its particular situation, identify the severity of the impacted resources, and develop a prioritized course of action. A simple and prescriptive remedy cannot be applied uniformly to every situation. However, basic principles and recommendations exist that strengthen security postures and reduce damages. ICS will assist State Agency staff in the development of mitigation plans based on investigation and incident response activities. At a minimum ICS will guide each agency through the following for mitigation planning:

Mitigation Measure Determination and Layering

Once vulnerabilities to the security program have been identified, ICS will help agencies determine the necessary risk mitigation measures to be put in place to create multiple layers of security. These integrated security controls will be designed to counteract, avoid, or minimize risks. The list of mitigation measures is almost endless and includes both physical protections, such as locks and alarms, and logical protections, such as automated intrusion detection logging and alerts. ICS is experienced in creating layers that are dynamic, cost-effective and that layered integration is maintainable.

Cyber Security Framework

Once the mitigation measures have been chosen by the agencies, and the approach to layering measures is approved, ICS will assist agencies in composing a plan that adheres to trusted principles. ICS guidance for mitigation planning includes many industry standards and best practices, but, typically adheres to the NIST principles for a tiered approach to risk mitigation. The Tier definitions are as follows:

Tier 1: Partial

- Risk Management Process - Organizational cyber-security risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program - There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- External Participation - An organization may not have the processes in place to participate in coordination or collaboration with other entities.

2(D) MITIGATION PLANS CONTINUED

Tier 2: Risk Informed

- Risk Management Process - Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cyber-security activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Risk Management Process - Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cyber-security activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program - There is an awareness of cyber-security risk at the organizational level but an organization-wide approach to managing cyber-security risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cyber-security duties. Cyber-security information is shared within the organization on an informal basis.
- External Participation - The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

Tier 3: Repeatable

- Risk Management Process - The organization's risk management practices are formally approved and expressed as policy. Organizational cyber-security practices are regularly updated based on the application of risk management processes to changes in business/ mission requirements and a changing threat and technology landscape.
- Integrated Risk Management Program - There is an organization-wide approach to manage cyber-security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- External Participation - The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Services for State and Local Agencies

In the rapidly changing world of e-government, state and local agencies have an increasing need to integrate comprehensive strategy and cutting edge security into information operations as well as compliance with state and federal regulations such as HIPAA, IRS-1075, NIST, COBIT and/or ISO standards.

Compliance requirements and the looming risk of an IT security breach mean agencies must adopt preemptive strategies to protect their customers' sensitive data – fast and cost effectively. With new information security threats discovered daily, the challenge to meet these stringent demands has become increasingly difficult. In order to contain costs and increase efficiencies, many agencies are considering I.T. consolidation, data leakage protection, and data center optimization projects. While these efforts may help reduce costs and increase security, they require a trusted IT security and consulting firm to ensure success.

The ICS team is vigilant in their approach to information operations and technical security. ICS consultants stay abreast of current legislative requirements, regulatory compliance issues and industry best practices to meet the specialized information security needs of public sector agencies. You can rest assured that ICS has what it takes to ensure secure delivery of your organization's critical information infrastructure and keep operations flowing smoothly.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Technology Consulting

Vulnerability Assessment

You can't fix what you don't know is broken, and it is impossible to ensure the security of your network without a clear picture of its strengths and its weaknesses. Regularly scheduled vulnerability assessments are an uncomplicated way to uncover potential hazards.

There are countless individuals and entities intent on accessing other organizations' network resources and data for myriad reasons, and they're using the latest technology and techniques to accomplish this goal.

Without adequate protection, your organization can be easily compromised, resulting in anything from a minor inconvenience to a breach that seriously harms your operations and your bottom line. ICS can guide you through the process to properly safeguard any weak or exposed areas with an internal or external vulnerability assessment.

By working with ICS you:

- Catalog and prioritize vulnerabilities within your infrastructure.
- Implement quick, efficient and cost effective remediation solutions, created for your specific needs.
- Give your customers confidence by ensuring their information is secure.
- Satisfy regulatory compliance requirements.

Contact us today to get started.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ICS Inc.
Integrated Computer Solutions

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

The Current Risk Landscape

- Organizations which depend upon information systems are challenged by serious threats that can exploit both known and unknown vulnerabilities in systems.

- Threats include targeted attacks, operational disruptions due to natural disasters, human and system errors, and structural failures.

- These potentially harmful activities can compromise the **confidentiality, integrity,** or **availability** of information being processed, stored, or transmitted by information systems, resulting in adverse impacts on the organization, its operations, assets, and people, and endangering other organizations and national interests.

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Federal	State/Local	Commercial
September 19, 2012 **United States Navy** Washington, District Of Columbia Records exposed: **200,000**	October 26, 2012 **South Carolina Department of Revenue** Columbia, South Carolina Records exposed: **6.4 million**	October 8, 2012 **TD Bank** Cherry Hill, New Jersey Records exposed: **260,000**
August 2, 2012 **Environmental Protection Agency** Washington, District Of Columbia Records exposed: **7,800**	April 27, 2012 **Office of the Texas Attorney General** Austin, Texas Records exposed: **6.5 million** from the Texas voter database	September 19, 2012 **Blue Cross/Blue Shield of Massachusetts** Boston, Massachusetts Records exposed: **15,000**
June 16, 2012 **U.S. Department of the Interior National Business Center** Denver, Colorado Records exposed: **7,500**	May 12, 2012 **California Department of Social Services** Riverside, California Records exposed: **701,000**	November 16, 2012 **Nationwide Mutual Insurance Company and Allied Insurance** Columbus, Ohio Records exposed: **28,000**

The Ponemon Institute's 2010 U.S. Cost of a Data Breach found that the average organizational cost of a data breach in 2010 was $7.2 million. This was the equivalent of $214 per compromised record, markedly higher when compared to $204 in 2009. Ponemon's Cost of a Data Breach report is based on the actual data breach experiences of 51 U.S. companies from 15 different industry sectors.

www.privacyrights.org

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

[Case Study]

What do agencies/firms REALLY do when they have a breach?

THE CLIENT:

State Agency

- 2,500 Employees
- Serving 2-3 Million citizens
- Systems open to data sharing arrangements with sister agencies

THE BREACH:

250,000 social security numbers accessed by a third party on the web

THE RESPONSE:

State law required notification of the individual whose data was exposed.

- Agency performed extensive data validation to validate addresses, names, eliminate duplicates, etc.
- Agency prepared and mailed 250,000+ letters, 10% of which were returned and had to be retained by the Agency.
- 15 agency staff members met for 1 hour twice per day for 60-90 business days during the breach mitigation. (This is equivalent to 1,800 man hours or one man year.)

[Case Study, Cont.]

What do agencies/firms REALLY do when they have a breach?

THE COSTS:

- Hard Cost 1: Data validation expense: $100,000
- Hard Cost 2: Letter preparation, materials, mailing (250,000 letters): $500,000
- Hard Cost 3: Returned letter storage (approx. 10-15% return rate): $1,000/mo
- Hard Cost 4: Vulnerability Scanning/Web Application Risk Assessment: $125,000
- Hard Cost 5: Credit Monitoring: $0 *(Agency chose to accept risk of future litigation)*
- Productivity Cost: 1,800 man hours x $54/hour (average employee expense) = $97,200
- Reputation and Opportunity Costs: Unknown

PROACTIVE RESPONSE CHOICES:

1. **BUDGET:** Put $1M - $3M in annual budget to anticipate a small to large breach.
2. **ASSESS:** Conduct an independent third party assessment for $30,000 - $100,000 depending on the size of your organization. Plan to spend 3% of your IT budget on security.
3. **DO NOTHING:** Pay a little now or pay ***a lot*** (10 – 100x) later.

! This situation exists in your organization today. Which proactive response choice will you make?

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

IT-Related Risk Management

Managing risk appropriately provides tremendous business value, as it helps improve all facets of information security.

Risk Management can help:

- Improve operational efficiency.
- Free up resources for new business initiatives.
- Ensure projects are delivered on time and within budget.
- Avoid IT service interruptions.
- Quickly identify IT security breaches.
- Maintain regulatory compliance.

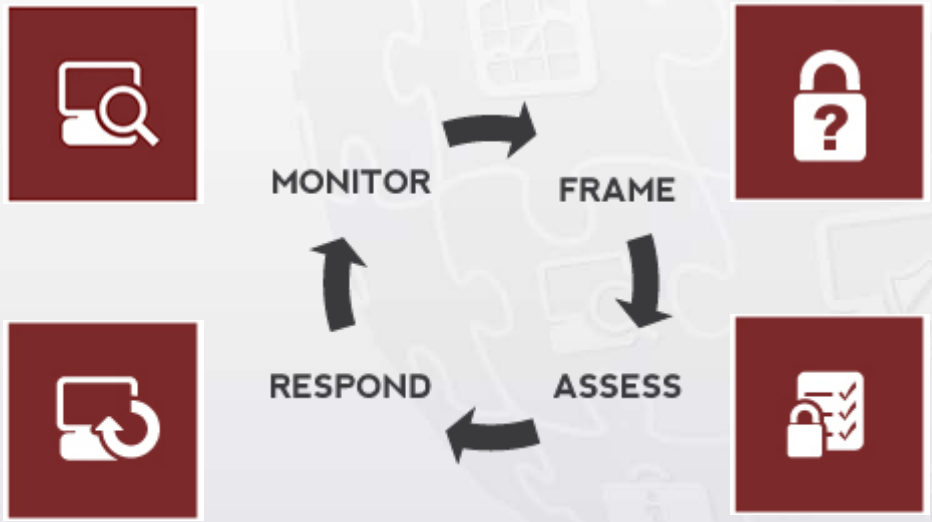
Principles of Risk Management

An organization's approach to risk assessment and risk management must always align with overarching enterprise objectives, and IT security goals must be based on overall enterprise risk management objectives.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

IT-Related Risk Management

Managing risk is a comprehensive and complex process that involves many activities and functions of an organization – its programs, investments, budgets, legal and safety issues, inventory and supply chain matters, and security.



ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Framing Risk

People at all levels within an organization have a role in managing information security risks to the organization's missions and business functions and the information systems that support those missions/business functions.

All organizations, from the largest to the smallest, whether in public or private sector, can profit from Risk Management. Appropriate risk management benefits all levels in the command chain. For example:

- **Boards and executive management** are empowered to make informed risk-aware decisions and guide organizations in a manner that allows risk to be managed effectively.
- **Corporate risk managers** are able to take a more comprehensive approach to enterprise risk management.
- **IT directors and security managers** are able to integrate IT-related risk management into overall enterprise risk management.
- **Enterprise governance officers** achieve a more complete IT governance perspective.
- **Business managers** save resources with proactive risk management efforts.

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Framing Risk

Attention must be given to **balancing the costs and benefits** associated with managing and mitigating risk.

Risk management is **an ongoing process** based on documented procedures that must constantly evaluated and updated for maximum efficacy.

Collective Risk

An integrated approach to managing risk brings together **the best collective judgments of individuals and groups within the organization** who are responsible for strategic planning, oversight, management, and day-to-day operations.

Everyone within the enterprise must be committed to operating within documented risk tolerance levels, and must be **held accountable** for their actions.

! **Remember:** one unlocked door, one open window, one unsuspecting user, **one inadvertent mistake is all it takes to allow a devastating breach**.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Assessment

- Evaluate current information security policies and procedures and assess overall IT security.
- Provide baseline for measurement of risk across the enterprise.
- Identify and prioritize security mitigation strategies.
- Direct activities to increase security controls in existing and future infrastructure.

Risk Assessment Benefits

A Comprehensive Risk Assessment provides a thorough evaluation of your organization's current IT security posture. The assessment will show you where the potentially weak areas are, in order of priority, and what needs to be done to secure those weak areas.

Effective Risk Management provides clearly defined guidelines for managing IT-related risks organization-wide.

- Leverage existing IT infrastructure investments
- Integrate with overall risk and compliance requirements
- Create a sense of accountability and risk ownership throughout the organization

DID YOU KNOW? ICS has conducted more than 150 comprehensive Risk/Security Assessments using industry best practices and standards.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Assessment

- Risk Management
- Security Planning
- System & Services Acquisition
- Certification & Accreditation
- Personnel Security
- Physical & Environmental Protection
- Contingency Planning
- Configuration Management
- Maintenance
- System and Information Integrity
- Media Protection
- Incident Response
- Awareness and Training
- Identification and Authentication
- Access Control
- Audit & Accountability
- System & Communications Protection

Balancing Risk and Value

An Information Security Risk Assessment provides a detailed evaluation of your organization's current IT security posture and recommendations to secure your information infrastructure.

The assessment will:

- expose potentially weak areas, in order of priority;
- identify what steps should be taken to secure weak areas; and
- provide roadmap of activities for the organization over the next 12-24 months.

It is then up to your organization to determine an acceptable level of risk and where to allocate additional resources to begin the process of implementing needed change.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Response

If a risk is determined to exceed organizational risk tolerance levels, a risk response action should be taken.

This may include:

- Avoidance
- Transfer of the risk
- Acceptance
- Risk mitigation

NOTE: Cost factors include the cost to mitigate, as well as the cost to the organization if no action is taken.

Risk Response Options

The response options should be prioritized and conducted according to the organization's risk action plan. The appropriate response will be based on resources, including cost factors, time constraints, human resources, and the ability to implement an effective and efficient response. Having a trusted IT partner in place will minimize costs associated with the extemporaneous responses often associated with risk mitigation.

Risk Tolerance Threshold

What is your risk tolerance threshold? How does your risk management strategy align?

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Response

The ICS ISRA process is based on National Institute of Standards and Technology (NIST) 800-53 and International Organization for Standardization (ISO) 27002:2005.

Our Information Security Risk Assessment Program provides an evaluation of an organization's current security posture and includes recommendations to secure and protect your valuable information and technology infrastructure.

An Acceptable Level of Risk

Risk and value should be considered along side one another. Risk is inherent in all organizations—it cannot be entirely avoided—therefore, risk and value must be considered simultaneously.

A Risk Assessment will provide a clear view of weak points in your organization. This knowledge will allow you to determine **how much risk is tolerable**. Once that has been determined, we can begin the process of systematically securing your network from breach.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Monitoring

An information security risk assessment is a thorough evaluation of your organization's current IT security posture and results in detailed recommendations on how to secure your information infrastructure.

A risk assessment should be conducted at least every three years, or when a major change to the system has occurred.

Benefits of Risk Monitoring

The results of risk assessments inform risk management decisions and guide risk responses.

To support the ongoing review of risk management decisions, organizations should **maintain risk assessments by incorporating any changes detected through risk monitoring.**

Risk monitoring provides organizations with an ongoing capability to determine the effectiveness of risk responses, to identify risk-impacting changes to organizational information systems and their operating environments, and to verify compliance.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Monitoring

Monitoring and assessing selected security controls on a continuous basis, documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to organizational officials are all critical to IT governance.

Risk Monitoring - Governance

Effective IT Risk Management assists in the governance of Information Technology.

The Risk Management process should be strategic and proactive, beginning with an evaluation to **determine risk tolerance.** This should be followed by a thorough **documentation of risk policies** and **regularly scheduled risk assessments** to evaluate risk factors and maintain risk standards.

Efficient IT Risk Management results in a positive ROI on the security investment.

ESTABLISH RISK TOLERANCE

DOCUMENT RISK POLICIES

MAINTAIN RISK STANDARDS

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Risk Self Assessment

Take this brief Risk Self Assessment to determine your organization's exposure level and need for a third-party risk assessment.

1. Does your organization have policies and procedures specific to information security?
2. Does your organization provide security training upon hire and annually after?
3. Does your organization conduct internal risk assessments annually or external risk assessments every 3 years?
4. Does your organization have an incident response team or plan?
5. Does your organization have a documented and tested disaster recovery and business continuity plan?

! **Note:** if you answered no to *any* of the questions above, you should consider a third-party Risk Assessment from ICS or another qualified comprehensive Risk Assessment provider.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

A Business-Minded Approach

It is crucial to choose a firm with a security-focused information technology background, that is business-minded and understands the delicate balance between risk management, value management, and process management.

Many of the costs associated with information security can be reduced by simply taking a systematic and proactive approach.

A Risk Assessment from ICS is based on relevant standards, including NIST, ISO, COBIT, and HIPAA. Our proven (and proprietary) project management methodology allows for a focus on **risk-based decision support** and **cost reductions in your security program**.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

ICS, Inc. is a **Security-Focused, Business-Minded IT Solutions Provider** with years of experience providing information assurance, technical support, advisory assistance, and operational services. ICS is unique in its market because we have an established track record of providing enterprise technology and security services to clients in the commercial field, public sector and education markets, as well as a foundation in service with the United States Department of Defense.

Streamline information security efficiency efforts.

The ICS team of skilled information security and technology professionals understands the complexities involved with protecting critical enterprise information and maximizing efficiencies.

Maximize information security budget.

Many of the costs associated with information security can be reduced simply by taking a systematic and proactive approach and working with qualified professionals that are security-focused. Let ICS show you how to maximize the return on your enterprise security investment.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

Integrated Risk Management

Balancing Risk and Budget

Founded	1997		
Headquarters	Montgomery, Alabama		
Project Sites	• Montgomery, Alabama • Tallahassee, Florida • Denver, Colorado	• Mechanicsburg, Pennsylvania • San Antonio, Texas	
Employees	• Heavily degreed • Professionally trained	• 100% hold one or more industry certifications • 70% with security clearances	
Solutions	• Risk Assessment • Business Continuity | Disaster Recovery • Technical Security • Solutions Management • Incident Response | Forensics	• Staff Support | Augmentation • Project Management • Information Assurance • Advisory & Assistance Services	• Network Operations • Enterprise Computing Services • Network Protection Services: • Offense | Defense | Operations
Performance Management	• Project-Based Cost Accounting System • Project Management Methodology with Earned Value Management		
Clients	• College Center for Library Automation of Florida • Tallahassee Community College • DeKalb County Schools (GA) • Duval County Public Schools (FL) • Carolina-Central Piedmont Community College (NC) • Medical University of South Carolina • Mississippi State University	• Alabama Supercomputer Authority • Alabama State Treasury • Florida Dept of Employment Opportunities • Florida Dept of Transportation • Georgia Technology Authority • Mississippi Dept of Employment Security • Texas Dept of Information Resources • North Carolina Health & Human Services • North Carolina State Treasurer	• State of Tennessee Nashville and Davidson Counties • Lee County Port Authority (FL) • Montgomery Water Works (AL) • Orange County, North Carolina • City of Troy, Alabama • Choctaw Indian Tribe (MS) • Mobile County Health Department (AL)

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Policy Development

Well-established IT policies can help ensure an optimal network environment in which data is stable, secure, and available. Effective IT policies can also help ensure operations continue under adverse situations, such as a natural disaster or other unplanned event.

ICS can work with your organization to create clearly defined IT policies and procedures that provide a framework for treating information as real property to be protected from unauthorized access, modification, intrusion and destruction.

Policy and standards development can include items such as:

- Information Security and Privacy
- Information Classification
- Information Security Infrastructure
- Acceptable Use
- Security Awareness and Training
- Access Control
- Password and Authentication
- Compliance
- Personnel Security
- Risk Management
- Physical and Environmental Security
- Third Party & Business Associates Security
- Network & Systems Operational Security
- Mobile Computing and Telecommuting
- Incident Response and Reporting
- Intrusion Detection and Prevention
- Malicious Software
- Information Systems Acquisition, Development and Maintenance
- Internet and Email Security
- Contingency Planning
- Retention Archiving and Disposition
- Business Continuity Planning (BCP) Security
- Remote Access – Mobile Computing
- Removable Media

A well-written IT Policy will serve as a best practices handbook for all employees within the organization and encourage their participation in preventing information breaches. These policies will help ensure controls are in place to protect information and will set the tone both internally and externally with regards to the importance of protecting your organization's information.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

CyberSecurity | Audit & Assessment

Penetration Testing

There are risks to your system everywhere, so the best way to keep your network safe is to let us hack it. ***Yes, you read that right.***

Penetration testing is often referred to as ethical hacking. In this test, our certified ethical hackers take the basic vulnerability assessment a step further, verifying the findings of the vulnerability assessment and the impact a breach could have in your external and internal networks.

When we're done, we will create a custom solution information security solution, tailored specifically for your organization.

Penetration testing should be performed bi-annually as an integral part of your larger security plan.

Following the penetration test, the organization will have a much clearer understanding of the weak areas within the IT infrastructure, as well as how to shore up defenses to protect the organization from a costly, potentially devastating security breach. This thorough test provides answers to the questions raised by the vulnerability assessment, and is an invaluable component of a comprehensive cybersecurity evaluation.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Information Assurance / CyberSecurity

ICS has been delivering information assurance, information protection and cyber-security services since 1997. The service catalog was initially developed to support our Department of Defense clients and has evolved to provide a military-grade level of service to our commercial and public sector clients.

- ***Programmatics*** (policy, planning, PMO support, risk based decision support);
- ***Risk Assessment*** (NIST 800-30; ISO 17799 / 27001 / 27002);
- ***Compliance*** (FISMA, COBIT, COSO, HIPAA, Governance, PCI DSS);
- ***Business Continuity Planning*** (BS25999; NFPA 1600; plan lifecycle management)
- ***Disaster Recovery*** (ISO/IEC 24762:2008; full lifecycle management);
- ***Technical Security*** (computer network defense / offense CND/CNO, attack & penetration; application security assessment; database security testing; system hardening);
- ***Solutions Management & Integration*** (design, source, build, deploy, manage);
- ***Incident Response*** (imaging, analysis, forensics, legal support).

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Incident Response (Post-Event)

Organizations that are dependent on information systems are challenged by serious threats that can exploit both known and unknown vulnerabilities in systems.

In the event of an information security emergency, the ICS Incident Response team will step in to help your organization identify the source of the compromise, preserve critical information, and prevent the spread of contamination or unauthorized access to other systems and networks.

Our on-site emergency response efforts will not cease until the incident has been eradicated and the systems and networks have been restored to normal operation.

ICS will provide knowledge transfer and reporting so your internal personnel are equipped to maintain protection of your information assets after the event.

Let ICS' Emergency Response Consultants act as your primary response team.

Related Services Include:
- Incident Response Planning
- Disaster Recovery Planning
- Forensics

To learn more about CyberSecurity services from ICS, visit our website at www.ICSInc.com.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Forensics

ICS offers forensic services to discover, analyze and document information in both proactive and reactive forensic circumstances. Many of our clients have found this service to be vital during personnel action, court order, civil action, and incident response situations.

Evidentiary Integrity
ICS has the knowledge and experience needed to achieve successful electronic evidence and data collection, protect evidentiary integrity, and provide factually accurate supporting documentation. As a technology security firm, we are well-qualified in this field and often provide supporting forensics documentation for clients to present to agencies such as the Department of Homeland Security, the Federal Bureau of Investigation, and state investigation agencies.

Litigation Support and Expert Testimony
ICS also provides litigation support with expert testimony in the event of court proceedings or prosecution.

Forensic Process:

Define Requirements: During the first phase of the forensics process, ICS will assess the situation and define the requirements of the project. This process often begins with a phone call in the middle of the night; the ICS team is available 24/7/365.

Data Collection: ICS will begin data acquisition, obtaining log files, imaging hard drives, and other data collection processes as soon as possible. In many cases we are on-site almost immediately; in other cases a court order must be obtained before data collection can begin.

Data Analysis: During the data analysis phase, ICS will sift through the data and process it in forensically sound manner. Thourough reports with supporting documentation are prepared.

Data Sharing:T he data sharing phase is the time when all of the findings are presented to the client in a detailed and clear presentation that can be used to prepare for legal proceedings, if necessary.

It is our hope that your organization will never require ICS forensics services; however, should the need arise, we are prepared to act as your primary response team.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Disaster Recovery Planning

Would your organization be able to continue critical business functions following a significant unplanned disaster? Or would an unexpected natural disaster or political event shut down operations entirely? Disaster Recovery Planning allows an organization to establish steps to continue operation at planned levels of service, despite events or interruptions.

Today's political and environmental climate requires that an organization be prepared for just about anything. ICS utilizes time tested Disaster Recovery Planning methods based on the standards established by the Disaster Recovery Institute International. We combine these industry standard best practices with our own proven proprietary processes in Disaster Recovery Planning to allow business operations to resume following virtually any unplanned event, whether natural or man-caused.

Services Include:

- Strategic Recovery Planning/Development
- Backup and Recovery Strategy
- Selection of Alternate Facilities
- Alternate Site Operations Planning
- Vendor Alignment
- Knowledge Transfer/Staff Training

Let ICS help your organization mitigate financial, physical and operational risk through the development of a comprehensive Disaster Recovery Plan. For organizations with existing BC and DR plans, experts recommend that an organization test their plans every year and update them every three years.

ICS will save you time and money by reviewing your organization's current strategies, documentation and plan readiness. We evaluate these based on industry standards and best practices and recommend improvements to help ensure successful continued operations in the face of an unexpected crisis.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Continuity of Operations Planning

Effective Continuity of Operations Planning will help ensure the security of your staff, visitors, and operations in the event of a crisis. In just 60 days, ICS will have your organization prepared to continue operations in virtually any unplanned event – from a minor interruption to a major disaster.

ICS' certified Continuity of Operations planners will help your organization develop appropriate resilience strategies, recovery objectives, business continuity, and crisis management plans. These plans can be implemented in collaboration with an integrated and comprehensive risk management initiative for maximum efficacy.

ICS Business Continuity:

- Federal Emergency Management Agency (FEMA) and US Guidelines (FCD-1 and CGC1)
- ISO 22301 Business Continuity Management Systems
- ISO 27031 Information Technology (Business Continuity)
- National Fire Protection Standard (NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs)

Services include:

- Plan Development
- Business Impact Assessment (BIA)
- Gap Analysis Studies
- Hazard Analysis Studies
- Plan Testing
- Alternate Site Operations Planning
- Knowledge Transfer/Staff Training

Let ICS prepare your organization with a comprehensive Continuity of Operations Program that integrates all of the necessary procedures required to execute contingency operations. Contact us today.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

A COMPREHENSIVE APPROACH TO

CYBERSECURITY

Surely no one left the keys in the front door... did they? What about other (less obvious) access points on your network? Do you know if confidential corporate and customer information is at risk? There's only one sure way to find out—by taking a comprehensive approach to information security.

- Risk Assessment
- Vulnerability Assessment
- Penetration Testing
- Web Application Assessment

ISO 9001:2008 Certified

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213

A COMPREHENSIVE APPROACH TO

INFORMATION SECURITY

We all know that information security is not merely as simple as locking the front door and setting the alarm.

A well-managed information and technology security strategy must be based on a comprehensive set of security assessments that provide a clear picture of your organization's network security posture and definitive steps to defend your network and data from unauthorized access.

If that sounds out of reach, it's time you took a look at ICS. Our information security assessments take a strategic, integrated approach to protecting your organization's valuable information and technology infrastructure.

ICS Inc. Integrated Computer Solutions
ISO 9001:2008 Certified

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213

STEP 1: RISK ASSESSMENT

An Information Security Risk Assessment provides a detailed evaluation of your organization's IT security posture, covering everything from configuration management to media protection to audit and accountability. Consider it like checking the doors and the windows on your network.

A Risk Assessment from ICS, Inc. will provide your organization with an objective overview of the security of your information infrastructure.

[STEP 1: RISK ASSESSMENT]

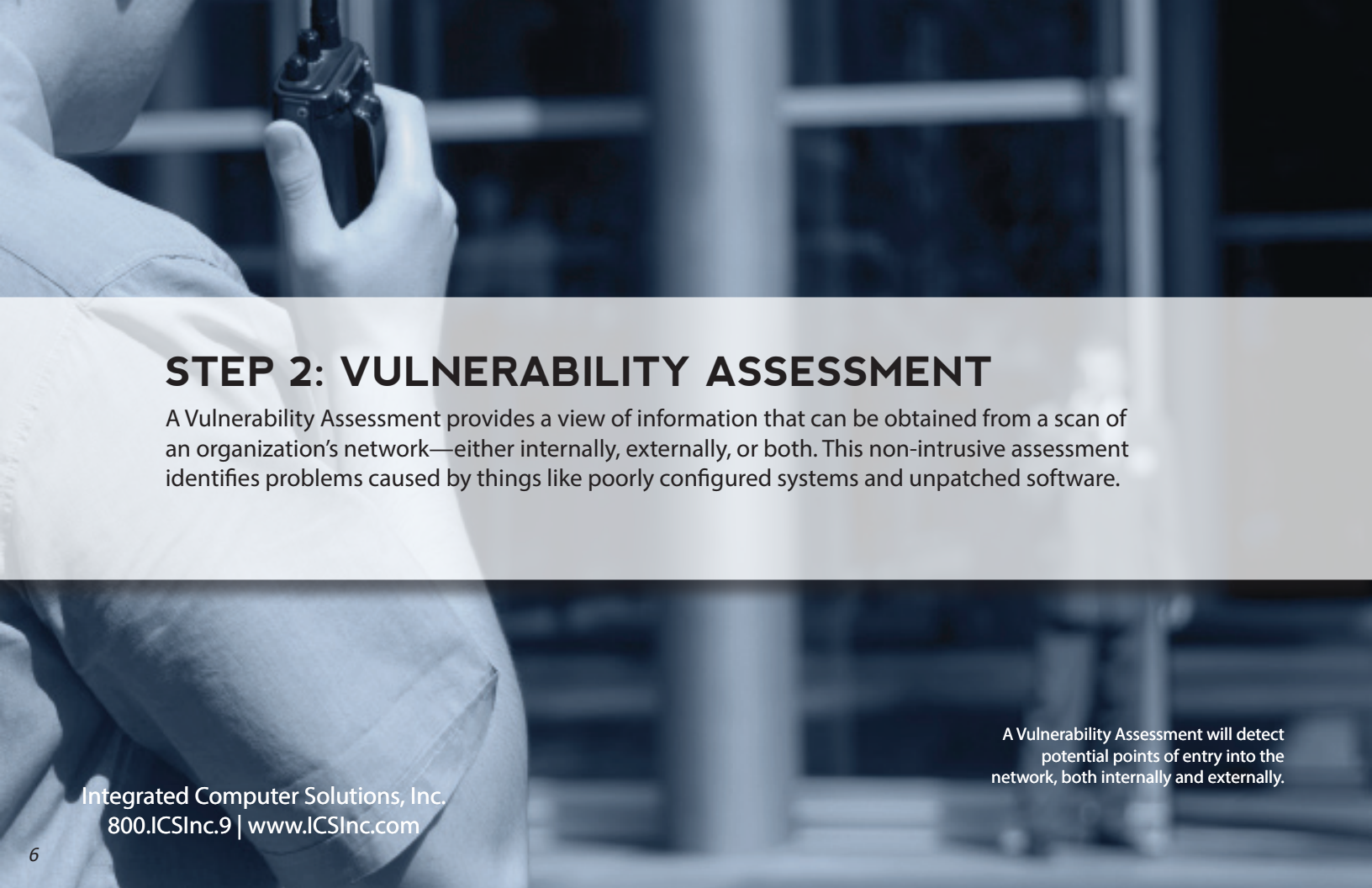
The fundamental first step in an information security health check is a Risk Assessment. A Risk Assessment is a thorough analysis of your organization's network infrastructure that will reveal weaknesses and provide a detailed plan to aid in securing the environment.

A Risk Assessment provides your organization with the information necessary to begin to implement an effective IT security plan. You will be able to prioritize the steps in the remediation plan based on business impact, determining which items need to be addressed immediately, which are less urgent, and which are not urgent at all. You will then have a solid foundation on which to build as you allocate resources to shore up network security defenses.

ICS Risk Assessment Services include:

- Risk Assessment Planning
- System & Services Acquisition
- Certification, Accreditation & Security Assessments
- Personnel Security
- Physical & Environmental Protection
- Contingency Planning
- Configuration Management
- Maintenance
- System and Information Integrity
- Media Protection
- Incident Response
- Awareness and Training
- Identification and Authentication
- Access Control
- Audit & Accountability
- System & Communications Protection

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213



STEP 2: VULNERABILITY ASSESSMENT

A Vulnerability Assessment provides a view of information that can be obtained from a scan of an organization's network—either internally, externally, or both. This non-intrusive assessment identifies problems caused by things like poorly configured systems and unpatched software.

A Vulnerability Assessment will detect potential points of entry into the network, both internally and externally.

[STEP 2: VULNERABILITY ASSESSMENT]

Without adequate protection, your organization's enterprise network could be compromised, resulting in anything from a minor inconvenience to a breach that could seriously harm your operations and your bottom line. A Vulnerability Assessment provides a clear picture of areas that could be intentionally or unintentionally exploited by authorized users or attackers, along with a strategic plan so you can defend your network.

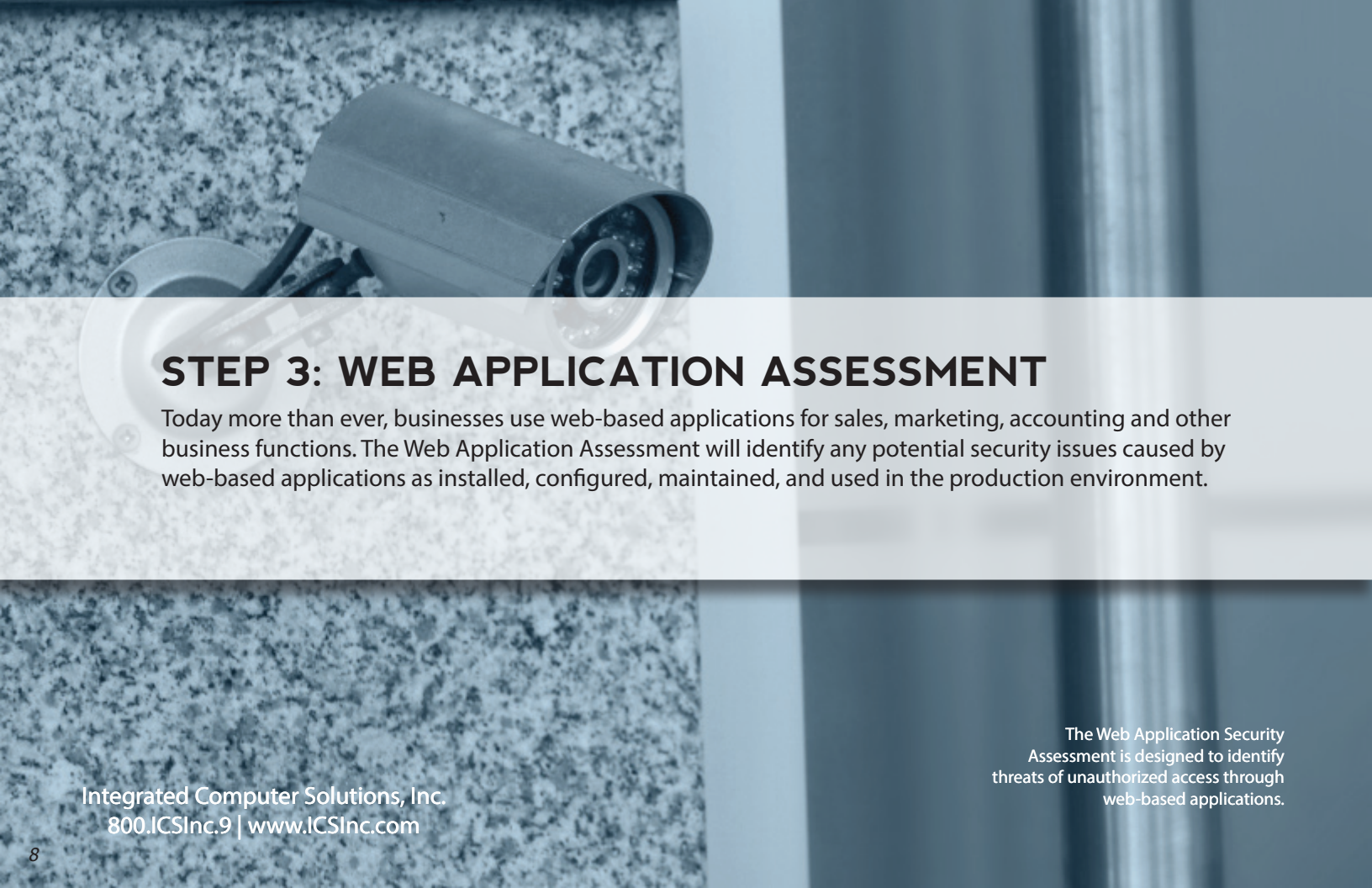
The Vulnerability Assessment utilizes non-intrusive scans of your organization's hosts, services, ports, protocols and known vulnerabilities that are evident from inside and/or outside the network. The assessment identifies, quantifies and prioritizes weaknesses caused by things such as unpatched or obsolete software and improper system configuration.

The following types of checks are involved in the Vulnerability Assessment:

- Patch Management
- Default user accounts
- Misconfigured Email, FTP and web servers
- Discovery of open ports and host OS discovery
- Denial of service (DOS) vulnerabilities
- Buffer overflow vulnerabilities
- Back doors and virus infected hosts
- Peer-to-peer, chat, and suspicious services

The Vulnerability Assessment includes a remediation strategy; however, it should be followed by a Penetration Test to determine the business impact of exploited vulnerabilities.

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213



STEP 3: WEB APPLICATION ASSESSMENT

Today more than ever, businesses use web-based applications for sales, marketing, accounting and other business functions. The Web Application Assessment will identify any potential security issues caused by web-based applications as installed, configured, maintained, and used in the production environment.

The Web Application Security Assessment is designed to identify threats of unauthorized access through web-based applications.

[STEP 3: WEB APPLICATION ASSESSMENT]

How many web-based applications does your organization use? Chances are good that you them for standard business functions in just about every department. These applications have many benefits, including the convenience of online accessibility and enhanced team collaboration; however, they can also expose an organization to vulnerabilities that could be leveraged to gain unauthorized access to network resources and sensitive data.

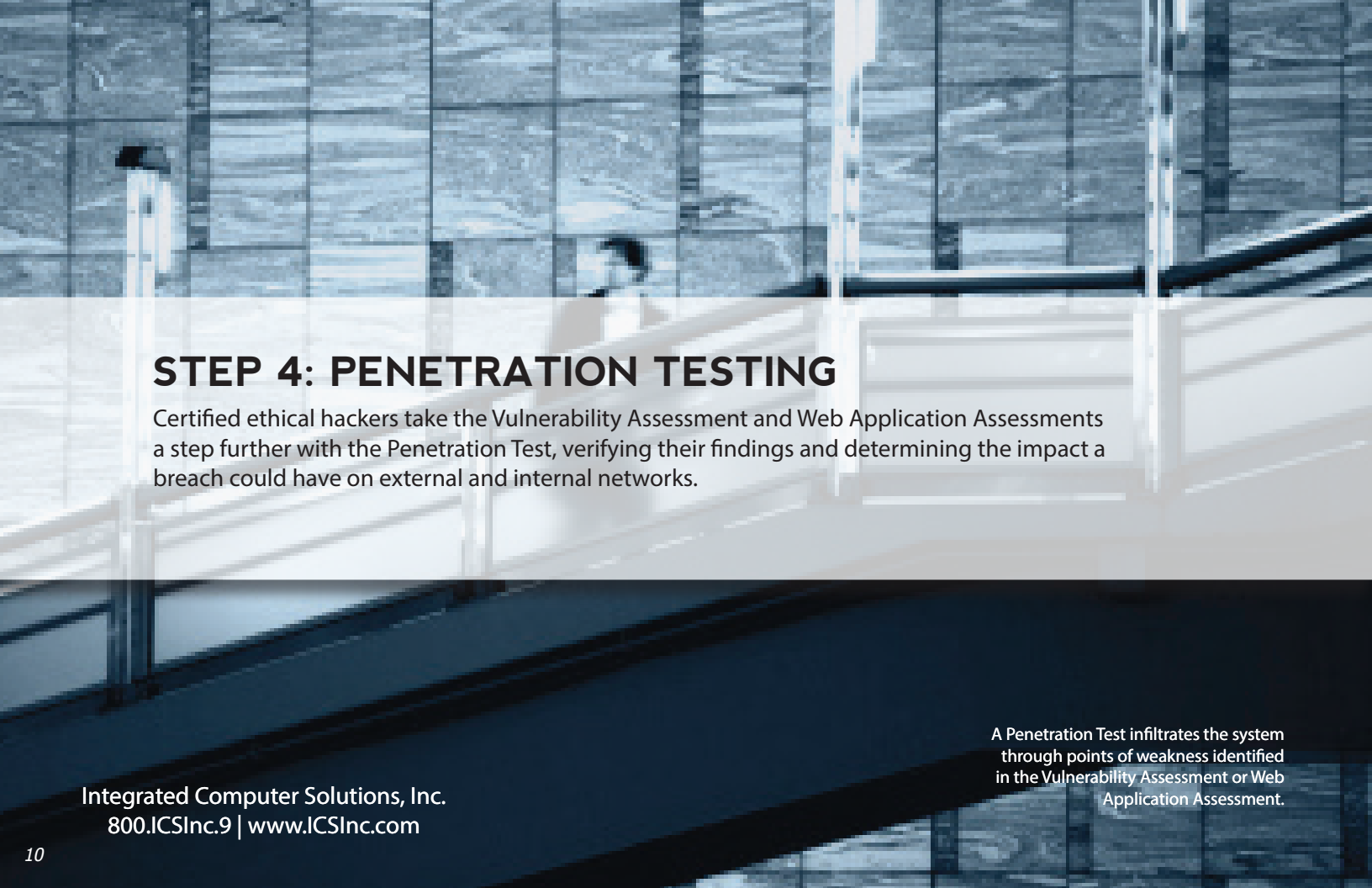
The primary goal of the Web Application Assessment is to identify security issues and weaknesses in the web-based application as installed, configured, maintained, and used in the production environment. A Web Application Assessment will identify threats of unauthorized access so you can keep sensitive information secure, no matter how many web-based applications your organization runs.

Examples of the types of security issues evaluated in the Web Application Assessment include:

- Input/Output validation (e.g., cross site scripting, SQL Injection)
- Application logic flaws (e.g., authentication bypass)
- Server configuration errors/versions (e.g., directory traversal, missing patches)

Web Application Assessments should be performed at least annually and anytime a new application is added. Like the Vulnerability Assessment, a Web Application Assessment should be followed by a Penetration Test to verify findings and determine the business impact of exploited vulnerabilities.

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213



STEP 4: PENETRATION TESTING

Certified ethical hackers take the Vulnerability Assessment and Web Application Assessments a step further with the Penetration Test, verifying their findings and determining the impact a breach could have on external and internal networks.

A Penetration Test infiltrates the system through points of weakness identified in the Vulnerability Assessment or Web Application Assessment.

[STEP 4: PENETRATION TESTING]

Often referred to as ethical hacking, a Penetration Test takes the basic Vulnerability Assessment or Web Application Assessment a step further by attempting to simulate an attack by a malicious user.

Using the information gained in the Vulnerability Assessment or Web Application Assessment, our certified ethical hackers attempt to infiltrate your organization's network through previously identified points of weakness. If the attack is successful, the technical security consultant will examine the effects of the attack and assess the impact an information security breach could have on your organization.

Penetration testing:

- verifies potential vulnerabilities
- validates security measures (e.g., IDS/IDP)
- helps satisfy compliance requirements

The results of the Penetration Test are thoroughly documented and presented along with a detailed approach for mitigation. Following the penetration test, your organization will have a much clearer understanding of weak areas within the IT infrastructure, as well as how to protect against a potentially devastating security breach.

© 2011-2013 Integrated Computer Solutions, Inc. All rights reserved. Rev. 1213

Integrated Computer Solutions, Inc.
800.ICSInc.9 | www.ICSInc.com

ISO 9001:2008 Certified

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

CyberSecurity | Audit & Assessment

Code Review

ICS is available for code review projects with the goal of identifying security issues and weaknesses in the applications' coding. We are able to conduct a systematic review of applications in scope for code review, which can include in excess of 1,000,000 lines of code.

Examples of programming languages involved are:

- .NET 3.5 framework
- VB.net
- ASP.NET
- C#
- Javascript

By conducting a static review of application code as it exists at the time of the assessment, we are able to provide an assessment of each application's architecture from a security perspective as well as remediation recommendations.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Business Continuity Planning

Effective Business Continuity Planning will help ensure the security of your staff, visitors, and operations in the event of a crisis. In just 60 days, ICS will have your organization prepared to continue operations in virtually any unplanned event – from a minor interruption to a major disaster.

ICS' certified business continuity planners will help your organization develop appropriate resilience strategies, recovery objectives, business continuity, and crisis management plans. These plans can be implemented in collaboration with an integrated and comprehensive risk management initiative for maximum efficacy.

ICS Business Continuity:

- Federal Emergency Management Agency (FEMA) and US Guidelines (FCD-1 and CGC1)
- ISO 22301 Business Continuity Management Systems
- ISO 27031 Information Technology (Business Continuity)
- National Fire Protection Standard (NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs)

Services include:

- Plan Development
- Business Impact Assessment (BIA)
- Gap Analysis Studies
- Hazard Analysis Studies
- Plan Testing
- Alternate Site Operations Planning
- Knowledge Transfer/Staff Training

Let ICS prepare your organization with a comprehensive Business Continuity Program that integrates all of the necessary procedures required to execute contingency operations. Contact us today.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114

ISO 9001:2008 Certified

CyberSecurity
Technology Consulting
Application Services
Staff Recruitment & Augmentation

At ICS, we pride ourselves in our unique ability to integrate comprehensive strategy and cutting edge security into information operations. Learn more at www.ICSInc.com.

Audit & Assessment

Our IT Audit and Assessment services provide you with independent, unbiased assessment of your security program, policies,and controls. Your executive leadership and management team can have confidence that your organization is adequately mitigating risk in alignment with business objectives.

ICS utilizes the best tools available in the market, coupled with our proprietary software and processes to save our clients time and unnecessary expense. Because ICS serves hundreds of clients every year, you will benefit from our significant investment in industry-leading technologies for services such as:

Risk Assessment
Know where you stand with a detailed and comprehensive assessment of your organization's security posture from ICS. Risk Assessments from ICS include invaluable strategies and recommendations to secure and protect your organization's information and technology infrastructure.

Vulnerability Assessment
A vulnerability assessment is an unobtrusive way to identify risks which may stem from unpatched or obsolete software, poorly configured systems, or inadequate security protocols. ICS will identify areas that are potentially exploitable and guide you through the steps needed to secure those weak areas.

Penetration Testing
A penetration test (pen test) takes the vulnerability assessment a step further, as an ICS certified ethical hacker attempts an actual attack on the points of weakness identified in the vulnerability assessment. The pen test will give you a clear understanding of how an actual attack could undermine your organization.

Web Application Assessment
Virtually all organizations today employ web-based applications for sales, marketing, accounting, and other standard business functions. A Web Application Assessment will uncover vulnerabilities that exist in web-based applications and provide strategies to maximize your system security.

Code Review
ICS is available for code review projects with the goal of identifying security issues and weaknesses in the applications' coding. We are able to conduct a systematic review of applications, which can include in excess of 1,000,000 lines of code.

Integrated Computer Solutions, Inc.
60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@icsinc.com • www.ICSInc.com

©2014 Integrated Computer Solutions, Inc.
Rev. 0114