Integrated Risk Management

Balancing Risk and Budget

ICS Inc.
Integrated Computer Solutions

ISO 9001:2015 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

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.

Integrated Risk Management

Balancing Risk and Budget

2012 Data Breaches by Sector

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**

Source: www.privacyrights.org, Chronology of Data Breaches. Updated January 13, 2013

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.

[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?

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.

BENEFITS OF RISK MANAGEMENT

ENABLES TECHNOLOGY

IMPROVES PROJECT DELIVERY

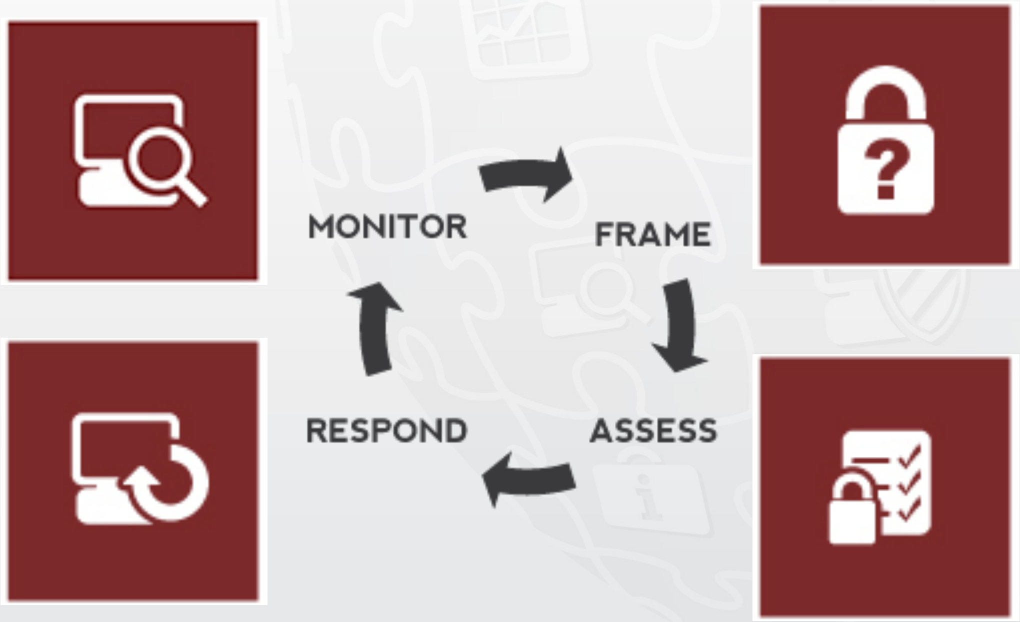
MINIMIZES DOWNTIME

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**.

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.



Managing risk is a comprehensive process that involves many activities and functions of an organization.

It includes:

- Framing Risk
- Assessing Risk
- Responding to Risk
- Risk Monitoring

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.

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**.

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.

Risk Assessment

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.

- 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

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

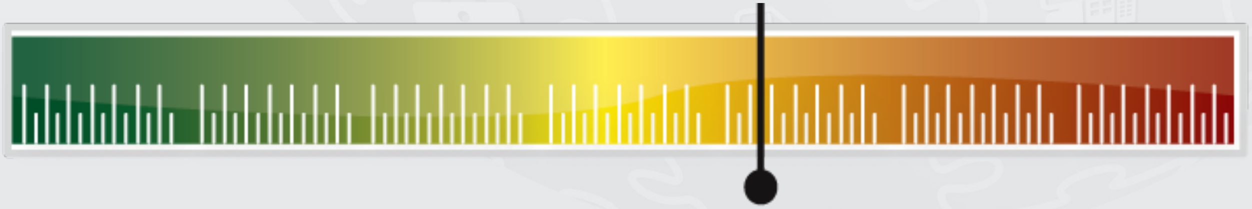
NOTE: Cost factors include the cost to mitigate, as well as the cost to the organization if no action is taken.

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?



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.

RISK
BUDGET

ANALYZING RISK

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.

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

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.

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**.

Integrated Risk Management

Balancing Risk and Budget

About Integrated Computer Solutions, Inc.

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.

ISO 9001:2015 Certified

Integrated Risk Management

Balancing Risk and Budget

About Integrated Computer Solutions, Inc.

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)

ICS Inc.
Integrated Computer Solutions

ISO 9001:2015 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