Ingalls Professional Services & Consulting

Ingalls considers professional services to be the backbone of our company. We offer a full suite of technology-enabled, integrated cybersecurity risk management services that can be customized for any business or organization. Our team of expert consultants focus on multiple service areas that find and fill gaps in your current security strategy, assess and test to identify risk, and develop comprehensive security solutions including:

Core Services and Capabilities

- ✓ vCISO
- ✓ Information Security Policy Development
- ✓ IT Business Continuity and Disaster Recovery Plan Development
- ✓ Risk Assessments

- ✓ Incident Response Readiness
- ✓ Social Engineering and Security Awareness Training
- ✓ Vulnerability Assessments and Penetration Testing

Virtual Chief Information Security Officer (vCISO)

A Virtual Chief Information Security Officer (vCISO) is specifically designed for companies who want a comprehensive information security program but lack the resources to hire a dedicated security team or IT security officer.

Key Benefits:

- A team of expert cybersecurity consultants that possess real-world skills and decades of experience your information security program needs to be successful

- Customized vCISO services tailored to each clients' needs

- A focus on understanding your needs to effectively develop and implement an information security program that is right for your organization

> " Our goal in providing Professional Services is to help our clients build a tailored and comprehensive risk management program.
>
> **– Scotlyn Clark**, Director of Professional Services at Ingalls "

Risk Assessments

Ingalls Information Security's risk assessment is the critical first step in determining where your most significant risks are, helping you recognize where resources should be invested.

Key Benefits:

- A deep dive into understanding your business processes; technology and information environment; technical, administrative, and physical safeguards; and compliance requirements

- Assessment of your company's risk based on the threats, attacker capabilities, and system vulnerabilities

- An in-depth risk assessment that identifies areas of risk, the magnitude of potential loss, and the probability that loss will occur.

Information Security Policy Development

Every organization needs a suite of security policies designed to keep information secure, detail guidelines on breach recovery and response, and articulate security controls. Ingalls ensures that Information Security policy requirements are aligned with business requirements while fully considering people, processes, and technology, no matter the stage of your policy development.

Key Benefits:

- Reasonable and appropriate guidance to assure the confidentiality, integrity, and availability of information resources

- Mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks, and computer systems

- Reputation protection as well as legal and ethical responsibility satisfaction

IT Business Continuity and Disaster Recovery Plan Development

An IT Business Continuity and Disaster Recovery Plan (BCDRP) focuses on maintaining the organization's mission/business processes during and after a significant disruption.

Key Benefits:

- An actionable solution to prepare for the impact of a broad range of threats including natural disasters, accidents, and technology-related hazards such as hardware failure
- A plan that provides a quick, calm, and efficient response in the event of an emergency
- Detailed guidelines that enhance your ability to quickly recover from a threat or breach

Business Impact Analysis

A Business Impact Analysis (BIA) is key to implementing business continuity and disaster recovery controls and to the contingency planning process. BIA results determine how critical an organization's systems are to the supported mission/business processes, what impact the loss of each system could have on the organization, and the system recovery time objectives (RTO).

Key Benefits:

- Defined recovery priorities and resource dependencies for mission critical processes
- Specified recovery time and recovery point (RT/RPO) objectives for critical systems
- A BIA that informs contingency planning requirements needed to develop a comprehensive BCDRP
- An IRP that hastens recovery time and reduces damage from a security incident

> "
> Organizations of all sizes can be the target of malicious actors. SMBs are an ever increasing target, and compared to large organizations, are oftentimes less equipped to deal with incidents.
>
> **– Stephen Gutleber**,
> Senior Cybersecurity Consultant
> at Ingalls
> "

Tabletop Testing

Tabletop Testing (TTX) is a hands-on interactive experience that simulates a real crisis, and it's up to you and your team to navigate it and practice expedient coordination and mobilization, incident investigation, identification of gaps in the IRP, and risks requiring mitigation in the Incident Response process.

Key Benefits:

- Full scale testing of an IRP
- Hands-on training that helps gauge and improve readiness in the event of an actual attack
- Ingalls provides you with a detailed post-TTX summary report that details recommendations and areas for improvement. Any and all questions are encouraged to ensure clarity and success

Social Engineering and Security Awareness Training

In any organization, the weakest security link is often the level of employee awareness. Insecure password management, tailgating through entrance doors, and interacting with malicious emails all expose a network to compromise. Ingalls can mimic these threats to test your organization's level of defense.

Key Benefits:

- Ingalls performs simulated social engineering that evaluates the knowledge employees have of social engineering tactics, as well as employees' ability to successfully identify and respond

- Ingalls will manage interactive, browser-based initial, remedial, and annual training to ensure that employees are able to recognize or react appropriately to information security threats and incidents

Vulnerability Assessments and Penetration Testing

Ingalls Information Security performs vulnerability assessment and penetration testing in order to provide tailored recommendations and reports to help you defend your infrastructure against hackers, cybersecurity attacks, and other malicious threat actors.

Key Benefits:

- Real-world techniques and knowledge to identify and exploit security vulnerabilities that could result in a breach of your security

- Ingalls helps you understand your company's effectiveness in surviving an attack by identifying any gaps, effectiveness of security measures in place, and if your system will detect and actively defend against attacks

Enabling Innovation Through Better Cyber Risk Management

Ingalls Information Security provides technology-enabled, integrated cybersecurity risk management services. Since 2010, Ingalls' diverse experience across military/defense intelligence, network security, information technology, and cybersecurity solutions has honed a powerful edge in preventing and responding to cyberattacks. Ingalls' expertise focuses on four business lines of service: Managed Detection and Response, Incident Response, Professional Services, and Government Programs. The company's core focus is to establish Louisiana as a cybersecurity center of excellence, and bring 5,000 industry jobs into the state.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452