

INFORMATION ASSURANCE SERVICES

Intekras's Information Assurance division offers a broad suite of solutions designed to protect your most critical information assets and reduce the probability or impact stemming from an undesirable or unexpected event. From identifying and ranking vulnerabilities and threats to recommending where and how to mitigate the most serious business, operational, and technical exposures, *Intekras* is uniquely qualified to assist you in protecting and defending your information and information systems from all IT risks.

Certification and Accreditation (C&A)

Intekras's C&A reviews are tailored to the relevant system development life cycle phase and program strategy and scaled according to the size and complexity of the system(s). Rather than regard C&A as simply a compliance exercise, we base our review upon a foundation of risk acceptance and management, by determining the risk to operations, assets, or individuals and the acceptability of the risk weighed against the mission or business needs of the agency/organization. Our C&A reviews allow for risk-based decisions about the information system's operation and can ensure that the system maintains the accredited security posture throughout its lifecycle.

Disaster Recovery/COOP

Intekras is well-versed in the issues associated with complying with Continuity of Operations (COOP), Continuity of Government (COG), Homeland Security Policies, and the carrying out of mission accountability at all times. From performing a Business Impact Analysis (BIA) to assessing and improving your COOP and providing testing services, our experts are able to assist in the mitigating of continuity risk.

Incident Response & Digital Forensics

When faced with resource misuse, policy abuse, denial-of-service, or data breach, *Intekras* consultants can immediately be dispatched to investigate the circumstances behind the event and provide assistance in remediation. We're able to retrieve key data buried in documents and memoranda, organize data contained in disparate digital information sources, investigate the incident while complying with Federal Rules of Civil Procedure and eDiscovery processes, and work with in-house counsel and law enforcement to assist in the identification and prosecution of perpetrators.

Independent Verification & Validation

The size of most information technology programs means they are fundamentally complex, risky, and difficult to manage. *Intekras* provides the visibility and tools needed to proactively ensure the success of the programs - from beginning to end and at every stage in between. *Intekras* consultants - skilled in such disciplines as project management, systems analysis, business process design, and risk management - seek to determine whether a solution (either in development or production) meets expectations and to identify where the project risks lie.

IT Governance Risk Review

The management of risks is a cornerstone of proper IT governance. *Intekras* helps to establish the organizational structure and business processes you need to implement an effective, sustainable IT Governance Risk Management program. These services focus on policies, procedures, and techniques that have been proven in enterprises like yours. Experienced *Intekras* security consultants can guide you through every step in creating a risk-minded organization that not only safeguards your vital information assets but mitigates the likelihood and impact of IT failures.



INFORMATION ASSURANCE SERVICES (cont.)

IT Security Architecture Review

Risk experts no longer view security as a product or a solution, but as a “defense in depth” methodology that is incorporated across the enterprise. The best way to manage IT security risk is through a systematic, architectural approach that is built upon a standards-based security foundation. *Intekras* provides valuable expertise and experience in supporting your security design and implementation efforts. *Intekras*'s Security Architecture Review will comprehensively review the applications, network, servers, and services within an organization's environment and identify methods to enhance and improve system infrastructure and support - including both future and existing infrastructure.

IT Security Operations Review

Despite the sophistication of network or system security measures in place, the compromise of information confidentiality, availability or integrity can be traced to failures in operational processes. *Intekras* is able to apply accepted best practices and risk frameworks to ensure that all aspects and functions of the security operation run in the most efficient and effective manner, including Capability Maturity Model Integration (CMMI), Control Objectives for Information Related Technology (COBIT) and Systems Security Engineering Capability Maturity Model (SSE-CMM). We also are able to apply such frameworks as the International Organization for Standardization (ISO) 27000 series or the National Institute of Standards and Technology (NIST) special publication 800 guidelines when evaluating the effectiveness of a security operation.

IT Security Risk Assessment

Risk management has reached a new level of importance in the information age. The growth of networked information systems and Internet-based commerce creates a potentially dangerous environment. From trade secrets and proprietary information to troop movements, sensitive medical records and financial transactions, critically important data flows through these systems and networks. *Intekras*'s IT Risk Assessments utilize the most current risk frameworks such as International Organization for Standardization (ISO) 27000 series or the National Institute of Standards and Technology (NIST) special publication 800 guidelines to identify, analyze, and evaluate the most critical exposures and then recommend ways to treat (mitigate, transfer, or accept) those risks.

Penetration Testing

While many organizations may be aware of system or network vulnerabilities, a surprising number never perform “proof of concept” testing by simulating an attack from a malicious source. Given today's growth in breaches and other attacks, an active analysis - carried out from the position of a potential attacker - of system configurations, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures - is clearly needed. Through active penetration testing, *Intekras* IT security experts are able determine the feasibility of an attack and the amount of impact a successful exploit, if discovered, may have.

Vulnerability Assessment

Many organizations coping with the growth in systems and networks across the enterprise are sometimes unable to identify, quantify, rank and prioritize the extent of vulnerabilities across their infrastructures at the level and frequency demanded in today's perilous environment. *Intekras*'s experienced security personnel are able to perform an extensive assessment of these risks and review the organization's Incident Response capabilities, operational protocols, policies and procedures, and other compensating controls to determine the extent of damage that could result from a data breach or other security failure.

