



CORPORATE CAPABILITIES

SUMMARY

Founded in 1992, Secure Computing and Communications, Inc. (Secure C2[®]) is dedicated to the establishment and improvement of information security for its clients. Our success has resulted from ensuring that clients' organizational governance—and control—objectives are rationally met and reinforced, especially with respect to deployed information technology assets. Hallmarked by technological excellence and completeness of vision, our services yield an effective level of information security that is optimized towards economically meeting business objectives with an acceptable level of residual risk.

The tradeoff between information security and the usability/accessibility of information can bedevil an organization as new technology is adopted ... whether for competitive advantage or because the legacy infrastructure has become outdated. For any number of reasons, the implementation of Information Technology (IT) products often focuses exclusively on ensuring that desired functions and information are available to legitimate, authorized users. We provide the requisite understanding of technical security measures — both strengths and weaknesses — to ensure that the control of information can be proactively addressed. Success is ensured by linking information control objectives, especially those related to business goals and corporate governance, with users' requirements.

Secure C2's clients are U.S. Government agencies, non-governmental organizations (NGO), and private-sector corporations that desire expert support, ranging in scope from constructing and implementing a comprehensive framework for managing information risk, to conducting detailed technical analyses, constrained to only address specific factors in the IT environment. Our goal is to provide comprehensive, cost effective, and workable solutions, which provide maximum user convenience and functionality while meeting information control objectives.

CORPORATE STATUS AND FACILITY SECURITY INFORMATION

Secure Computing and Communications, Inc. is a service-disabled, veteran-owned, small business concern (SDVO SBC) with respect to the *Veterans Entrepreneurship and Small Business Development Act of 1999* (PL 106-50) as amended. This status is especially meaningful to organizations impacted by the *Veterans Benefit Act of 2003* (PL 108-183) and Executive Order 13360, *Providing Opportunities for Service-Disabled Veteran Business to Increase Their Contracting and Subcontracting*.

Secure C2 holds a Top Secret (TS) facility clearance (CAGE 02VE0). All technical staff have been cleared by the Defense Security Service for access to Top Secret information.

CONTACT INFORMATION

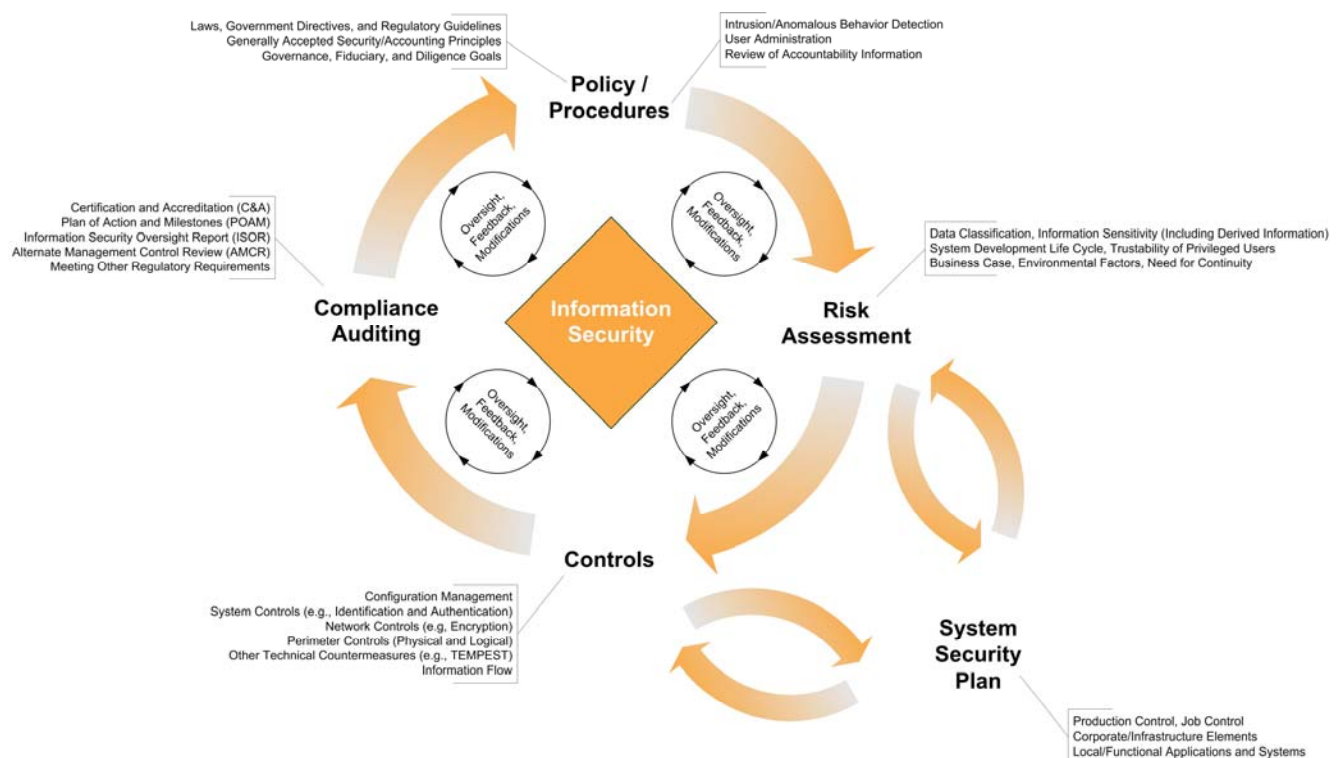
Secure Computing and Communications, Inc.
P.O. Box 551
Great Falls, Virginia 22066

Roger Sudduth, President
Phone: 703.244-5626

E-mail: SudduthRM@SecureC2.com
Fax: 703.759-4329

CAPABILITIES

Our expertise is centered on the management of information, in whatever form it might be. Generally, an organization already has a fundamental understanding of how its information should be controlled, as evinced by the manner in which paper copies of information are handled. Locked file cabinets, controlled distribution systems, archival storage and other attributes of printed information and other media provide a good starting point for establishing the control criteria for electronic information. Secure C2 excels in enabling your organization's understanding of the true value of its information. Our assistance in the identification and implementation of controls, where necessary, will ensure that the costs are commensurate with the information's value. We have a systemic approach to controlling information, paying special attention to your use of information technology products, as depicted in the illustration below.



Controlling Information, Supported by Secure C2 ... Your Oversight and Feedback Ensure Success!

We'd appreciate, and enjoy, the opportunity to describe to you in person the concepts summarized in the above diagram. Because of the variety of elements that are relevant to controlling information, the diagram might seem to be complex. Close attention to these elements — and ensuring their applicability to meeting business objectives and regulatory guidelines, while maintaining usability — ensures organizational success. After our discussion, we believe you will appreciate that information security can be less complicated than it appears at first glance to be.

Do contact us so that we can discuss your information, and your management objectives!

Another way to view Secure C2's capabilities, is to order them into the following areas:

- **Policies, Planning, and Programs.** Information is the lifeblood of an organization. The control and management of information can contribute to ensuring continued success, especially if these activities are not ad-hoc in nature. The establishment of policies should guide and constrain planning activities, which result in the programs that meet organizational goals. Secure C2's expertise is not confined to technology. Rather, the context of technology — and its multi-dimensional impacts on information within the existing organizational climate — is well understood.
- **Managing Risks.** Information is subject to misuse. This misuse could appear to be innocuous, such as one employee inadvertently learning private, personal information of another employee, or more sinister, like an employee attempting to divert organizational resources for financial gain. We are expert in analyzing information to establish its real value to the organization. In many cases, this value is expressed in terms of consequences of loss or disclosure, rather than a setting a specific dollar amount. Armed with an idea of the information's value, the risks to the information can be factored into every other aspect of information security, including ensuring IT operations are responsibly approved. Government clients recognize this aspect of our support as being crucial to the conduct of the security certification and accreditation program, to maximize the program's real value.
- **Security Architecture/Engineering.** To be effective and unobtrusive, the need for automated controls over data and information are ideally addressed early in the life cycle. Secure C2 has extensive experience in architecting security aspects of systems ranging from monolithic applications in a homogeneous processing environment to complex, distributed systems implemented across heterogeneous systems. Secure C2's support is tailored to meet your requirements. Included in this aspect of our service are the analysis and testing activities that support certification and accreditation determinations for government clients, and equivalent aspects of approving production operations in a corporate environment.
- **Implementation/Integration.** Commodity and proprietary applications, operating systems, and other technologies offer differing security services with which access to information, in its respective medium, can be controlled. Integration of these services when meeting information control objectives (such as ensuring operating-system security-services are employed, as practicable, instead of "homegrown" functionality in a proprietary application) can introduce artifacts into the organizational IT infrastructure that are difficult to resolve. Secure C2 has a wealth of experience in this regard, with expertise in technologies ranging from object request brokers, multilevel security (MLS), public key infrastructures (PKI), to the use of cryptography to enable secure access via the Internet.
- **Assessing Security Status/Active Defense.** Establishing controls over information and data is only part of the information life-cycle's security element; validating the controls' efficacy and monitoring also plays a crucial role. Based on organizational goals and applicable regulatory requirements, Secure C2 can assist your organization determine the optimal information security assessment strategy, including the identification and implementation of automated security assessment tools, and host- and network-based intrusion detection systems. We have expertise with the gamut of active defense measures ranging from perimeter firewalls, E-mail spam and content filters, to malicious software and anti-virus countermeasures ... and even more complex countermeasures, like automated anomaly detection or managed automated vulnerability assessment.

SOME REPRESENTATIVE SUPPORT ACTIVITIES

In the event it is easier to learn if our capabilities may meet your requirements by reviewing specific activities that we've undertaken for other clients, the following *representative* list should help.

Policies, Planning, and Programs

- Establishing and promulgating elements of laws and regulations that are applicable to operations;
- Crafting and articulating policies and procedures, including drafting documents like *Standard Operating Procedures* (SOP); and
- Assisting in planning to meet strategic/tactical objectives, such as by developing system and network *Concept of Operations* (ConOps) documents.

Managing Risks

- Identifying the sensitivity and value of data and information, including analyses to establish aggregation and inference problems in database and data-warehouse applications;
- Developing and participating in all aspects of the certification and accreditation process, in accordance with Intelligence Community directives and Defense organization's required methodology, including those with widespread applicability like the *Defense Information Assurance Certification and Accreditation Process* (DIACAP) and its predecessor, the *Defense Information Technology Security Certification and Accreditation Process* (DITSCAP), as well as uniformed service's unique standards, such as that contained in Army Regulation (AR) 25-2, *Information Assurance*.
- Similar support of the C&A process for civil agencies, and the equivalent processes for non-government entities, using the applicable methodology, such as the *National Information Assurance Certification and Accreditation Process* (NIACAP), agency-specific standards, such as described in the *Foreign Affairs Manual* that is applicable to the Department of State and other non-Defense agencies overseas; or *Generally Accepted Security Principles* or other standards for NGOs and corporations; and
- Defining and realizing programs related to the management of information, including continuity of operations (COOP) planning, contingency planning (CP), and production/job control.

Security Architecture/Engineering

- Analysis, requirements specification, and security advocacy for development/integration of security relevant aspects of IT architectures as well as component elements, like public key infrastructures (PKI), firewalls, and MLS guard systems, both high- and low-assurance ; and
- Analysis, requirements specification, and security advocacy supporting the development and engineering of proprietary application systems, including distributed systems with complex interprocess communications, such as mail-enabled data communications.

Implementation/Integration

- Deploying, configuring, and operating server-based and desktop malicious-software and anti-virus solutions, including Symantec and MacAfee products, as well as establishing server settings relevant to the control of such threats, including mail (SMTP) and domain name system (DNS) servers, and
- Deploying, configuring, and operating: filtering servers and appliances, like Clearswift's MIMESweeper and specialty products, equivalent open products like SpamAssassin, as well as additional technical solutions, including the use of Black Hole-type countermeasures.

Assessing Security Status/Active Defense

- IT security assessments of facilities, networks, and systems supported by automated tools, like Kane Security Analyst (KSA) and open alternatives, like Nessus Internet Security Scanner; and
- Engineering, deploying and operating intrusion detection/defense systems, like Enterasys Dragon IDS, CiscoWorks IDS components, and equivalent open-systems products like Tripwire and Snort.