

# Enterprise Security Risk Management



Securing Your Way of Life



## *Our Story*

### *Covenant Security Solutions' Mission: How Can We Best Serve You?*

*Covenant Security Solutions (CSS) is a woman owned 8(a) certified company founded in 2003 with the expressed purpose of providing security solutions to our clients based on the following principles:*

- *Respect: We at CSS never lose sight of the fact that we are teaming with our clients who are dedicated professionals and owners of the information assets. We value our client relationships, and fully understand the significance of our recommendations and findings on the impact of our client's data security.*
- *Shared Visions: CSS will provide our clients with the solution(s) needed, at an affordable cost. We will work with our clients to develop solution(s) that fully satisfy organizational or mission needs while providing a level of security that will represent a benefit and an asset, not a cost or a burden.*
- *Empowerment: The Covenant staff works with each of its clients to ensure that each service offering provides the customer with a means of assuming control over their own security by involving our clients, in each step of the process.*

### *How does Covenant Security Solutions Distinguish Our Value to Clients?*

- ***Leadership:** Thought leadership in the security arena. We at Covenant Security Solutions provide thought leadership to our community. Our staff includes Certified Information Systems Security Professionals (CISSPs') (90% of staff), along with several well noted security certifications to include Certified Pen Testing Experts (CPTe). Our staff have supported ISC2, been quoted in several noteworthy publications, and provided guidance on technical whitepapers. For example the President of the company has been published in the Defense Information Systems Agency (DISA), IA Newsletter, and interviewed on Federal News Radio on Amtower Off-Center Broadcast.*

- **Independence:** *Our goals and performance are tied to your security success. Covenant Security Solutions solely supports security related programs and projects. In keeping this focus, we come in with your security as the upmost priority. Our consultants are not influenced by divergent corporate objectives, tight budgets on the overall program, they are influenced by making sure you understand your risk and feel comfortable with the mitigation process.*
- **Strategic Alliances:** *Create value for your organization through niche (security) focused providers. We understand that real value to our client is not being the sole answer, but bringing the best knowledge and solutions that fit your goals. Covenant Security Solutions has built alliance with industry leaders and small niched providers to bring the “best answer” to the table. We’ve worked with companies such as Symantec, Northrop Grumman and RIAC LLC to name a few. From a global enterprise to small one person consultancy we aim to bring the quality, talent and solutions desired to effectively manage your enterprise risks.*



## Foundation

*It goes without saying that Information Technology is critical to your business or agency. Just imagine having to go through an entire workday without access to your data and you quickly realize how essential the availability of information is in meeting your customer’s needs and avoiding the cost of lost productivity. Similarly, imagine reading your e-mail at the beginning of the day and finding a stream of messages from someone thanking you for providing easy access to your client’s sensitive or proprietary information. What could be more damaging to your credibility or mission?*

*These examples make clear that it is important to proactively mitigate risk and exercise due diligence in securing your information infrastructure. The confidentiality, integrity and*

*availability of everything from customer contact information to proprietary mission-critical data is crucial to the success or failure of your organization.*

*One of the greatest paradigm shifts we must face in this new era is that risk is an inherent part of doing business. There is always going to be something we “don’t know” or never anticipated. This is especially true in the area of Information Technology. Everything from new software to the latest hardware gadget captures our imagination and faster than we can execute our Purchase Orders, this technology quickly becomes an inherent part of our mission(s). This rapid transition also brings with it a list of known and unknown risks that organization must now acknowledge and manage on a near real time basis.*

*The next paradigm shift in this new era of Web 2.0 and Web 3.0 is that our information can move and change truly at the “speed of light.” Information is now collected dynamically via blogs, social networking and wikis which allow for on demand and massive amounts of evolving data. This information can now have a life-span of importance going from critical to your organization to non-critical in a matter of seconds and days versus weeks to months. Often this means having a flexible security understanding. A risk methodology that can “move at the speed of light,” and be adaptive to continue to support your organization, while not carrying large security overhead costs for data that under this new paradigm may be obsolete or even more disconcerting, not protecting data at inception adequately enough due to lack of understanding of it’s importance.*

*We combine the above paradigm shift with an era in which the sophistication and commercialization of network attacks utilize the existing and hacker discovered vulnerabilities and weaknesses against our organizations. We are no longer in the era of the “script kiddie,” hacking for fun or just to be disruptive. Based on Symantec’s “Internet Security Threat Report, Volume XII, Published September 2007,” The following list describes the current threat landscape:*

- *Increased professionalization and commercialization of malicious activities*
- *Threats that are increasingly tailored for specific regions*
- *Increasing numbers of multi-staged attacks*
- *Attackers targeting victims by first exploiting trusted entities like social networks and*
- *Convergence of attack methods*

*More detail is outlined in their full report, however this is mentioned to validate the shift in understanding to the current threat space from just the disgruntled employee or group of bored geniuses to a level of planning and sophistication similar to any Fortune 500 company bringing a new business software line to market. The new era provides an affirmation of an old adage that “information is power.” Adversaries realize the competitive and monetary advantage that your information may bring to their situation or vantage point. This shift in the sophistication of the hacker and the corresponding attacks, has brought about a rapid change from modeling our risk efforts from a purely risk avoidance activity to a more holistic approach of risk management*

which encompasses the reality that threats are emerging, changing and receding, in many cases, faster than our organizations can change their policies to address the risk. The below matrix illustrates the differences in tactics employed based on the above scenario of risk avoidance versus risk management.

<i>RISK AVOIDANCE</i>	<i>RISK MANAGEMENT</i>
<i>Technology Driven</i>	<i>Process Driven</i>
<i>Perimeter Focused</i>	<i>Protection Focused on Mission Critical Assets and Processes</i>
<i>Legislative Compliance (NIST, SOX, DOD8500)</i>	<i>Risk Based Compliance (Business Impact, Global Insight, Shared Accountability)</i>

Therefore recognizing this shift in threat models Covenant Security Solutions’ is actively working with clients to shift focus in their organizations from just the protection of barriers and stove piped security processes to viewing it from an enterprise management approach and awareness. This awareness assists your organization in placing your resources appropriately while countering the potential to respond to threats in a “one-size-fits all” approach to security. This method of “one-size-fits all” is best noted when a general checklist is applied to all parts of your organization and all systems with little difference to the probability or likelihood of incident occurrence. The goal of an effective security program should be to identify and understand security controls from a larger organizational context based on the true value of the asset, information or process being protected.

In summary the person, organization or nation seeking the data that your agency/organization holds has become more sophisticated and the desire for data has increased. If security is viewed as an impediment to the mission or new market penetration then the risk is high that work around activities are in place which pose a great risk to the integrity of the network and as such the data that the organization is seeking to protect. Risk Mitigation through a reasoned and fully documented process ensures that senior personnel have an understanding of actions have consequences and that attempting to protect everything will equate to protecting nothing as the truly sensitive material will be treated the same as the mundane.



# Services

*How can we empower your Mission and help you Manage and Monitor evolving security risk across your enterprise?*

*We believe above all else in the golden rule: treat others as you would like to be treated. That means that you, as our client, are treated with all respect, courtesy, and care that we accord our own business. By adopting this philosophy we commit ourselves to seeking ideal tailored solutions from your perspective designed to address your organization's unique and specific needs, in everything from initial risk assessment to risk analysis to solution recommendation/implementation.*

*So how do we empower your mission?*

***F***irst we acknowledge the paradigm shift that is in our threat space. The assumption of working under solely a defense in depth or layered security paradigm with catch all checklists or scripts does not fit the reality of limited resources and the dynamic and fluid threats that rapidly evolve as identified in our Foundation Section.

*This understanding is further defined in our risk management practice to recognize that the security risks are inherently interrelated and affect not just the CIO and IT Department but rather the entire organization.*

***We at Covenant Security Solutions recognize and have developed our service model around the reality that security incidents may run across several departments from Human Resources to Finance, your supplier community and to mission related partners with whom you must share data. We therefore provide our information assurance services based on an Enterprise Risk Management approach that correlates your security support to its' impact on your mission and business/mission risk tolerance.***

**S**econdly, we provide a path from a risk avoidance model to a risk management model. This requires awareness that assets and processes should be ranked in order of importance to your mission and protection dollars should be allocated according to those rankings and risk severity. We also model risks based on probability of occurrence, likelihood of the occurrence and most importantly impact to your organization. These probabilities have a relational component which allows you to understand their impact across your enterprise.

***We have therefore developed a model of providing niche level expertise made up of our core staff with rapid reach to vetted complimentary service partners. This extends our capacity to meet your defined risk with much greater knowledge, depth and agility Our Information Assurance (IA) service offerings are our focus, not an adjunct to other service delivery offerings.***

**T**hirdly, we recognize that in assessing and managing security risks we best serve our client's interests as independent auditors. Most often organizations out of convenience or trust for the IT professionals on staff, then entrust the same organization to define and develop their security posture. The thinking is that they clearly know best our architecture and therefore should be responsible for security of that architecture. However, industry best practices and lesson learned carried over from the financial industry increasingly show this is not always the best arrangement. Independence is a key function of security. Often even the best intentioned IT professionals find it hard to be critical of their own organization and work. This critical view is key to an effective security program. Unfortunately, in many circumstances this becomes more of a popularity contest to show, "My network does not have vulnerabilities." When in most cases the opposite is true and risk avoidance is not the bar standard to be measured against, but rather leads to the downfall of many security programs. It is recommended by the ISACA, a leading IT auditor's association, the following two conditions should exist, especially in handling of IT audits:

**"03 Professional Independence**

*In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance.*

**04 Organisational Independence**

*The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment."*

*The principles outlined above define our approach and mission.*

***Our goal is to review risk globally, with the aim and focus of translating the client's corporate/mission objectives into a program designed to minimize the impact of an ever evolving threat space. Covenant Security Solutions is a proven provider with the independence from your organization and the professional standing that is critical to objectively and successfully review and mitigate your security risk.***



## **Enterprise Risk Management**

***We leverage our understanding of your challenges, enhancing our ability to help you address them while balancing your productivity and profitability with risk.***

*Covenant Security Solutions works closely with you to thoroughly analyze your organization's information to identify vulnerabilities and threats, and then develop a tailored management approach that is fully compatible with your existing capabilities in order to mitigate the exposed risks.*

*We provide a thorough review of your organization's actual and potential risks. Outlined below are the successful methodologies we employ:*

### ***Risk Identification, Assessment & Management***

- *Our process begins with a detailed automated software questionnaire. This automated process assists us in assessing your current security posture and modeling many varied possibilities and outcomes versus a traditional checklist. The questionnaire focuses on assisting the client in the identification of risks in several areas from technical controls to policy controls and, most importantly, the abilities of your personnel to sustain and implement your security process, as well as ascertain their current level of expertise. In addition, it provides assistance in aligning the identified risk to your business processes and goals.*
- *The assessment, once completed, will then provide us with a "road map" of security risk areas of concern that are classified as High Risk, Medium Risk, or Low Risk. The benefit of this is that it lets you identify exactly what security solutions or processes you need so that you can better balance your schedule and costs for implementing security within your organization and/or system. Also, it allows for the early identification of potential risk monitoring items required to maintain a balanced risk posture.*
- *The last step after identifying possible mitigation strategies is to formulate a management plan that will empower your organization in the support of mitigating security vulnerabilities and effectively monitoring your program's ability to maintain your desired security risk posture.*

*We provide the following services as components of the security risk management process:*

## ***Security Engineering***

*We assist organizations in managing security risk throughout the acquisition/procurement lifecycle. Our staff is highly experienced in supporting development environments throughout each phase of the systems development lifecycle.*

- ***Concept Exploration:*** Assist and facilitate in assessing near-term and long-term security impacts of specific system development ideas and assist in the early definition of Security Concept of Operations (SECONOP) and expected risks.
- ***Design/Development Phase:*** Assist and facilitate in the early definition of Security Architecture, allocation of current policy requirements at the component/sub-component level. Perform security trade studies for developer. Identify technologies for the developer which can balance security with cost and schedule. In addition, we support the design reviews and Program Office security personnel in meeting the requirements as set forth by your agency's Certifying Authorities.
- ***Fielding/Deployment:*** Assist with the creation of or provide system security testing documentation. Conduct system testing to include running security scans and executing specially-tailored, step-by-step testing procedures based on your risk model. In addition, we provide support for the documentation required by your organization's security audit processes.

## ***Security Policy Review & Development***

*We define and develop security policies for your organization based on current guidance, regulations, and industry best practices. Through every step of the process we put you first to ensure that your security policy is truly yours: a perfect fit for your organization. A brief sample of the types of documentation we have created successfully for our clients include:*

- *System Security Plans (SSP)*
- *Security Concept of Operations (SECONOPs)*
- *Security Requirements Traceability Matrix (SRTM)*
- *Trusted Facility Manual (TFM)*
- *Security Features User's Guide (SFUG)*
- *Contingency/Disaster Recovery Plans*
- *Software and Hardware Security Configuration Guides*

*Specifically for our Government clients we further tailor the above to meet the rigorous requirements of the Certification & Accreditation Process. The Covenant Security Solutions average consultant brings 10 years or greater in expertise to this field. Our security consultants have worked across the federal, defense and intelligence community and are capable of executing the following regulations:*

- *Department of Defense Intelligence Information System (DoDIIS) Certification and Accreditation Guide,*
- *Director of Central Intelligence Directive (DCID 6/3),*
- *NSA/CSS Information System Certification and Accreditation Process Guide (NISCAP).*
- *DoD Information Technology Security Certification & Accreditation Process (DITSCAP)/ now DIACAP and the DoD 8500.*
- *National Institute of Standards Special Publication (NIST-SP) 800 Series, eg. 53& 53A*

## ***Independent Security Assessment***

*Covenant Security Solutions provides your organization with management, documentation, and testing support for security auditing processes. Realizing that this can be a daunting task for even the largest and most seasoned organization, our staff works closely with you to organize your auditing tasks into easily manageable steps that will satisfy validating your security program and posture.*

*Our approach is to assist you in developing test procedures that are tailored to your risk needs. Rather than solely use pre-canned test scripts or scanners developed for quick base lining across multiple networks or systems, we develop procedures and test scripts centered around your system's capabilities that will show you and your Certifying Organization exactly how your organization shall meet the requirements, either through technical or policy controls.*

*In addition, these procedures are designed to be repeatable, step-by-step evolutions written in clear, non-technical English that can be run by anyone in your organization, and not just your technical staff, which provides greater ownership, lower risk and ultimately lower costs to risk maintenance.*

*We also focus our testing not just on the technical aspects of your organization, but also place considerable energy exercising the non-technical factors as well. We will develop procedures based on accepted nationally and internationally recognized Security Standards, such as the National Institute of Standards (NIST) or International Organization for Standardization (ISO). These procedures test the training knowledge of your staff, seeking to evaluate their understanding of your policies. Review of your agreements, memorandum of understandings, contracts etc. Do these agreements provide you with the protection required to hold vendors, clients and internal personnel accountable for information protection? These items are critical and CSS is committed to lowering organizational risk and going beyond a technical assessment of your IT infrastructure.*

*Lastly, we provide you with our test procedures in a soft-copy format that enables your on-site personnel to continue validating the system security and modifying the procedures as often as needed when major system changes occur. The testing documentation can support the following activities:*

- *Internal Security Audit Functions – This allows in the corporate suite, a Chief Security Officer (CSO), or in the government suite, a Program Information System Security Manager (ISSM) to provide testing on an ad hoc basis to developers, business continuity planners, including off-site testing of the organization’s baseline to ensure that security controls are continuing to be followed.*
- *Specifically for government clients this documentation is required to support the Security Testing & Evaluation (ST&E) and Certification Testing & Evaluation (CT&E) processes required under federal security policies and even more importantly, which can have an impact on agency funding as noted under the Federal Information Security Management Act (FISMA).*

## ***Penetration Testing & Intrusion Detection Services***

### ***Penetration Testing***

*Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers. Covenant Certified Penetration Testers perform these tests after careful consideration, notification, and planning has taken place and approval of a test plan, in conformance to the guidance provided in NIST SP 800-42 Guideline On Network Security Testing, by the client activity.*

*Penetration testing can be an invaluable technique to any organization's information security program. However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's networks response time due to network scanning and vulnerability scanning. Furthermore, the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable, even though the organization benefits in knowing that the system could have been rendered inoperable by an intruder. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated. Since penetration testing is designed to simulate an attack and uses tools and techniques that may be restricted by law, federal regulations, and organizational policy, it is imperative that formal permission for conducting penetration testing is granted prior to starting. Covenant Security Solutions’ works with our clients to provide appropriate Non Disclosure Agreements and Consent forms as required to ensure all parties are*

*in concurrence and aware of the activities being undertaken upon their request and any implications to their networks or operations.*

### ***Intrusion Detections Services***

*Covenant analysts provide visibility into the client security posture enabling client staff to maintain a situational awareness of the network and security infrastructure at all times. Covenant analysts provide the localization of content, information on critical emerging threats and vulnerabilities, and recommendations on activity in response to security incidents and threats to your network. Covenant deploys, monitors and maintains a Network Intrusion Detection System (NIDS) in accordance with NIST SP 800-94. Covenant works with client personnel to ensure that the following is addressed:*

- *Appropriate critical assets are protected*
- *Provide guidance and recommendations to ensure the efficient operation of sensors*
- *Ensure that sensors are deployed to see all information for appropriate network segments*
- *Provide deployment strategies for data that may be unfiltered (outside the firewall) and data that has been filtered (inside the firewall)*

*Covenant is accustomed to working with many types of network topologies. This experience of working with different network architectures is essential when planning sensor deployment. If networking topologies are not fully examined and sensors are improperly deployed, attacks can pass through undetected. Covenant follows best practices and good system administration to ensure that the network is effectively secured.*

### ***Security Education & Awareness Training***

*We provide both high-level and in-depth training for individual security processes, policies, and procedures tailored to your organization's specific needs, while providing the skills and knowledge needed to safeguard your organization's information.*

*Bearing in mind that one solution does not suit all needs, we focus our training offerings on each level of your organization, from executives and policy makers to system administrators down to your end users, with each offering focused on the specific knowledge needs of the target audience. Because we know that training does not take place in isolation from your overall mission, we make every possible effort to integrate our training solutions into our other service offerings. Not only does this allow you to make better use of your personnel and resources, it also empowers your staff with the knowledge and skills needed to fully implement and maintain your system security solutions.*

*Consistent with this belief in empowering you to control your own security infrastructure, we also provide instruction that "trains the trainer", enabling your own staff experts to perpetuate*

*knowledge among your workforce whenever and wherever needed. Depending on the mission needs and infrastructure of your organization, we can provide instruction in the form of conventional, classroom-centered training, hands-on technical training, computer-based individualized instruction, or a combination of all of these. While we tailor technical and subject-specific training to the needs of your organization, some of our basic security training service offerings includes:*

- *Basic Information Security Awareness*
- *Certification and Accreditation Policy Familiarization*
- *System Vulnerability Analysis and Remediation Techniques*

*These are only a few of the areas in which we can assist your organization in meeting its security needs. If there are any areas of special concern or technical expertise for which training is not already available, Covenant Security Solutions will tailor a class based on your risk management process to determine exactly what these needs are and construct training that is both practical and affordable.*

# *Contact Covenant Security Solutions*

*Our headquarters is located in the greater Washington, D.C. area and we are ready to meet your needs. If you are located outside of the D.C. area, we are more than capable of responding to your requirements. In an effort to empower and keep you the client at the center of our process, we use secure collaboration software, allowing you to view our progress and enabling us to include you in the review of documents or training developments from anywhere in the U.S.*

Ready? Please contact us below.

## *Point of Contacts*

*Mr. William Laramie, PMP  
Chief Operating Officer  
Phone: 866-824-8022 ext. 809  
Email: [info@covenantsec.com](mailto:info@covenantsec.com)*

*Or*

*Mr. Richard Kemp  
Alliance Manager  
Phone: 866-824-8022 ext. 817  
Email: [kemp\\_richard@covenantsec.com](mailto:kemp_richard@covenantsec.com)*