

Below we've described some of Consciere's recent projects to provide a sampling of our capabilities.

Service	Customer Vertical	Case Study Examples
GRC Program Services	Financial Services Technology Software Philanthropy Financial Services	<a href="#">Vulnerability Management Program Design/Implement</a> <a href="#">InfoSec Capability Maturity Assessment</a> <a href="#">GRC Software Content Integration</a> <a href="#">Information Security Program Roadmap</a> <a href="#">Regulated Information Asset Mapping and Controls Review</a>
Architecture Design	Health Care E-Commerce Retail	<a href="#">Enterprise Security Architecture Design</a> <a href="#">Mobile Security Architecture Review</a> <a href="#">Secure IT Environment Design and Implementation Support</a>
Infrastructure Assessment	E-Commerce Financial Services Retail Public Transportation	<a href="#">Enterprise Firewall Efficiency Analysis</a> <a href="#">VoIP Security Assessment</a> <a href="#">Firewall Configuration Audit</a> <a href="#">SharePoint Portal Security Review</a>
Application Assessment	Retail Financial Services Technology Financial Services Energy	<a href="#">Web Application Security Assessment</a> <a href="#">Source Code Security Review</a> <a href="#">Web Application Security Scanner Verification</a> <a href="#">Banking application security assessment</a> <a href="#">Customer Notification Web Application Review</a>
Compliance Consulting	Entertainment/Media	<a href="#">PCI Audit Preparation</a> <a href="#">Safe Harbor Compliance Readiness</a>
Incident Response	Local Government	<a href="#">Computer Forensics Investigation</a>
Staff Augmentation	Financial Services Entertainment/Media	<a href="#">Security Engineer &amp; Compliance Staff Augmentation</a>

## InfoSec Capability Maturity Assessment

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was asked to provide a capabilities maturity assessment for a large technology product company seeking to move into the software as a service (SaaS) market. Specifically, we focused on information and physical security requirements specified by our client's Fortune 500 customers, and capabilities that were being built to deliver on these commitments. We worked closely with our client to refine internal perspectives around security offerings through research into market trends in managed security services, clarified relevant contractual commitments, scored the current security program and offerings against a custom framework derived from the Capability Maturity Model, and presented a summary of results to the director of security services. Our work was instrumental in driving a renewed organizational investment in key areas such as policy development, compliance, intrusion monitoring/detection/response, and risk management.

## Vulnerability Management Program Design/Implement

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere's extensive experience was recently applied to develop a vulnerability management program (VMP) for a privately held financial services company. The project began with an assessment of current vulnerability management technology capabilities, processes, and people in order to design and document a best practices information security VMP. The program scope included patching, antimalware, security configuration, and unauthorized asset tracking for all information systems and applications. Beyond program assessment and development, Consciere also provided recommendations for reallocating key roles and responsibilities, developed key metrics to manage the program ongoing, and delivered requirements for an executive level dashboard. One of the key outcomes of our work was much greater intra-organizational alignment between business, security, and IT operations groups through intelligent leveraging of existing security capabilities and processes.

## Web Application Security Assessment

[\(Back to Top\)](#) [\(Request More Information\)](#)

As an example of numerous web application security assessments regularly performed by Consciere, we recently performed a 3-week assessment of a Fortune 500 retailer's web presence in both the US and Canada. The engagement began with on-site interviews of development team members, leading to remote, semi-informed ("gray box") manual penetration testing and automated scanning using a well-known commercial tool, followed by a post-assessment debrief with development teams. Consciere assessed over 865 URLs, and identified over 300 application-layer issues that were refined into 17 unique and systemic vulnerabilities. The highest-risk findings included unauthorized session impersonation, and systemic lack of output encoding resulting in numerous instances of cross-site scripting and other client-side injection vulnerabilities. The findings were well-received by the client's development teams, who appreciated the high quality of the analysis that exceeded previous testing of a similar nature by other consulting firms. The project sponsor also greatly appreciated the quality of the deliverable, calling it a "...nice read of our culture - high value, no fluff, straight and to the point."

## Safe Harbor Compliance Readiness

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere assisted a Fortune 500 media company with Safe Harbor compliance efforts in support of their international e-commerce presence. The organization had defined internal policies based on international security and privacy standards, which they used for evaluating their Safe Harbor compliance status. Consciere assisted IT and development team stakeholders to determine scope, provided expert guidance in interpreting and applying compliance requirements, helped further define standards where adaptation was necessary, created specific technology standards where gaps existed, and helped set criteria for acceptable evidence of compliance. Consciere also assisted with compliance lifecycle management, including regular engagement with control owners, escalation of issues, and drove resolution of open items and project risks. Over the multi-month engagement, Consciere's consultants identified and implemented multiple ideas to streamline and simplify the compliance management process, including centralized tracking of requirements, accountability, and status. Based on stakeholder feedback, Consciere's blend of technical and business experience enabled control owners and other stakeholders to meet their compliance obligations, gave management the visibility needed to make sound strategic decisions, and promoted the internal reputation of the information security compliance team who sponsored the project.

## Enterprise Security Architecture Design

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere recently led an initiative with a large managed health care provider to integrate security into their existing enterprise architecture practices. After conducting an aggressive campaign within the information security practice to ensure that the standards, practices, and policies were aligned with the compliance and business objectives of the organization, Consciere examined the enterprise architecture process and identified several ways to integrate security into the architecture cycle. Additionally, consultants demonstrated the newly adapted processes by producing a handful of new target architectures for security sensitive systems. This effort provided the tools and process for the organization to satisfy their internal security requirements in a design phase, as opposed to a costly and frustrating reactionary cycle.

## Enterprise Firewall Efficiency Analysis

[\(Back to Top\)](#) [\(Request More Information\)](#)

A major e-commerce presence recently leveraged Consciere to conduct an architectural analysis of their network security architecture. The organization had a long history of unprecedented growth and acquisitions, which had led to a sprawling network and firewall topology. Consciere conducted a comprehensive architectural analysis of the existing environment and determined that a redefinition of their network segmentation strategy would enable them to reduce the number of devices, increase performance, decrease management, and reduce access control rule counts without compromising the security objectives of the existing access control.

## Source Code Security Review

[\(Back to Top\)](#) [\(Request More Information\)](#)

Upon inheriting ownership of a legacy online commerce application from a 3rd-party developer, one of Consciere's financial services clients discovered indications of potentially serious application-level vulnerabilities and quarantined the application to a non-production environment. Consciere was subsequently engaged to conduct a source code security review of the VB.NET application in order to identify and mitigate high- and -medium-severity vulnerabilities before restoration to production status. The assessment included reviewing the results from automated security scanning tools

and manual source code review. Consciere's review found a number of security vulnerabilities in the application, including weak encryption, weak protection of sensitive application data, and endemic output encoding issues such as cross-site scripting (XSS). We then worked directly with the client's internal application development teams to develop and prioritize mitigations for each finding, and the application was subsequently restored to production status following implementation of necessary fixes.

## Computer Forensics Investigation

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was engaged by a municipal government entity to investigate large volumes of unsolicited email and other suspicious network activity that appeared to originate from municipality-owned computer systems and networks. The activity had left the municipality without Internet access and had severely impacted normal business operations. Consciere collaborated with forensics experts from two different firms to evaluate the municipality's computing environment; determine the scope and severity of systems affected; perform forensics-based root cause analysis; collect, analyze, and preserve relevant digital evidence in a manner that is legally admissible and in accordance with industry best practices; provide recommendations for remediation and guidance for relevant regulatory notification requirements. The suspicious network activity subsided and the municipality's Internet egress was restored after Consciere's team identified a handful of compromised systems, helped take those systems offline, and recommended firewall rule updates.

## Security Engineer & Compliance Staff Augmentation

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere has placed 5 full-time equivalent consultants at clients over nearly 2 years to perform information security engineering projects including: Active Directory Group Policy design, deployment, and troubleshooting to enforce Windows desktop and server security configuration standards; transition of security operations service desk ticket queue management to the network operations team; deployment and initial configuration of security appliances for network access control, IPS, SSL VPN, log correlation, and vulnerability management; PGP administration; Windows local privilege removal; web proxy client deployment and troubleshooting; network security zones and RBAC design; and firewall rule optimization. We've also placed 1 full-time equivalent consultant for multiple months to augment information security compliance team capacity to handle unexpected regulatory compliance staffing needs.

## VoIP Security Assessment

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was engaged to conduct a security design review, threat assessment, and formulate/execute a plan for testing security controls related to a new VoIP phone system deployment at a mid-sized financial company. Consciere identified 22 issues across 7 categories resulting in 11 specific recommendations for remediation. The review identified key oversights by telecom vendor and internal teams that resulted in reduced security control effectiveness and reduced reliability of enterprise disaster recovery facilities.

## PCI Audit Preparation

[\(Back to Top\)](#) [\(Request More Information\)](#)

Often Consciere is requested to advise clients on Payment Card Industry Data Security Standard (PCI DSS) compliance requirements and remediation strategies. An example of such an engagement is our recent review of a secure web payment services architecture at a mid-sized financial services firm to ensure that its design and implementation would support compliance with PCI requirements. The system was ultimately targeted for audit against PCI DSS, so it was a high priority for our client to understand in advance of a formal audit what potential non-compliance issues might arise and apply controls in advance. Consciere identified 12 instances of potential non-compliance during the review, and worked with the customer application development team to formulate practical recommendations for remediating all findings prior to service deployment.

## Banking application security assessment

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere worked with a federally-chartered financial institution to evaluate the security of an externally-developed banking application architecture, assess a non-production instance of the application for common vulnerabilities using manual and automated code review plus limited penetration testing, and test the underlying application infrastructure for basic security configuration best practices. Although Consciere identified issues including SQL injection and cross-site

scripting, penetration testing indicated the issues were very difficult to exploit due to compensating controls in the application environment. Consciere worked with the external application development company to prioritize and document recommended remediation actions, including implementation of output encoding and enforcing use of defined stored procedures.

## Customer Notification Web Application Review

[\(Back to Top\)](#) [\(Request More Information\)](#)

One of Consciere's mid-size energy sector customers requested an application security review, with the objective of turning the existing security review process from a series of one-off ad-hoc efforts into a repeatable process with consistent metrics over time. The client intentionally selected a small public-facing informational application for the pilot project, because it presented representative complexity and involved several internal groups, but posed non-critical risk to the organization. Consciere conducted a security review of the application, combining both best-practice areas of analysis as well as industry-specific performance requirements. Through an iterative review process, the review methodology was tuned not just to the specific application, but to all subsequent applications developed through a similar process, expected to operate in a common production environment, and exposed to similar threats. The process was subsequently used to improve the speed and accuracy of ongoing application security reviews for internally-developed or customized applications.

## GRC Software Content Integration

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was retained to assist a GRC software and services company to revise and expand its flagship product line. Consciere applied our expertise as security practitioners to help incorporate a series of well-known compliance frameworks into software content modules. End users of the software could then load the mix of module content customized to their organization's requirements, inventory their security controls, and leverage automated assessment, reporting and monitoring features. Consciere lead a team of subject matter experts in the development of frameworks for ISO 27002, the HIPAA Security Rule, and the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.2. For each requirement, the Consciere team identified the minimum and typical controls required for effective risk mitigation and/or compliance, and provided a mapping of functional control requirements to standards and directives within the frameworks. In addition, Consciere contributed to the larger effort of normalizing a catalog of security controls for use across multiple software modules. At the conclusion of multiple project phases, the client was able to release the software product and associated services more quickly than they could with internal resources, with a wider array of modules and more accurate data.

## Information Security Program Roadmap

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was asked to develop a 3-year roadmap to help set investment priorities for the enterprise security program at a large nonprofit philanthropic organization. We assessed existing operations and internal perceptions, gathered requirements across the enterprise, and consolidated the requirements into discrete tasks over the 3-year timeline. Consciere collected nearly 100 specific functional requirements tied to business drivers and processes. We leveraged our experience in both the private and the public/NGO sectors to identify high-priority activities, and illuminated key dependencies and redundancies. The result was a visually concise roadmap and supporting narrative documentation illustrating a set of immediate tasks over the ensuing 12-18 months, and clarified dependencies and priorities that enabled maximum flexibility over the full 36 month timeframe. The roadmap deliverables were subsequently used to drive strategy for the information security group, resulting in more consistent and effective delivery of services to internal IT customers and organizational units.

## Regulated Information Asset Mapping and Controls Review

[\(Back to Top\)](#) [\(Request More Information\)](#)

A mid-sized financial services company retained Consciere for a multi-phased engagement to map the flow of information governed by specific state regulations throughout the enterprise, and with external entities. In the first phase, direct observation and interviews were used to create a high-level map of groups and departments, and the types of information they exchanged. In subsequent phases, Consciere isolated a specific department for deeper analysis, identifying attributes for each major exchange of information, including flow parameters, security controls, trends in volume and frequency, and other aspects important for both technical security and compliance. Consciere refined the visual presentation of the information flows through several iterations, turning busy "spaghetti" diagrams into clear and maintainable representations with high information density. The client commissioned a plotter-sized printout to be hung in

the information security department to focus staff attention on key points of sensitive information handling, and to strategically target ongoing information security investments.

## SharePoint Portal Security Review

[\(Back to Top\)](#) [\(Request More Information\)](#)

One of Consciere's public transportation sector clients requested a security review of a high-profile initiative to drive greater customer information sharing via an Internet-facing Microsoft SharePoint portal instance. The review was segmented into two phases, including an initial architecture/design review, followed by penetration testing and vulnerability assessment of the eventual deployed application. Consciere quickly identified during the design review that the project significantly exceeded the organization's risk tolerance in several respects, and made the difficult recommendation to stop all development activity until critical security issues could be resolved. Consciere's recommendation was accepted, and the organization halted the portal initiative.

## Mobile Security Architecture Review

[\(Back to Top\)](#) [\(Request More Information\)](#)

A major e-commerce service provider asked Consciere to review the security architecture proposed in a series of technical patent applications. Consciere reviewed the security architecture and specific controls against a series of typical use cases and best practices for similar applications. By employing an independent assessment perspective, Consciere expanded upon the standard software security review process, and was able to identify security controls and methods with known flaws or specific failure modes, prior to further major investments by the client. The client was able to reduce risk through more robust security mechanisms, and reduce cost by focusing on development of a smaller number of stronger solutions.

## Firewall Configuration Audit

[\(Back to Top\)](#) [\(Request More Information\)](#)

Consciere was recently selected to conduct a firewall configuration review for a Fortune 500 retailer as part of their ongoing compliance obligations. Consciere's security engineers adapted the organizations technical standards into a series of simple audit and reporting tools, which provided repeatable and efficient methods to identify firewall configurations that were inconsistent with the organizations standards. Leveraging these automated tools, the assessment was completed in a fraction of the time a manual configuration audit would have required.

## Secure IT Environment Design and Implementation Support

[\(Back to Top\)](#) [\(Request More Information\)](#)

One of the nation's largest retailers recently looked to Consciere to assist in the architecture and deployment of a high security network infrastructure to isolate sensitive data and applications from the threats and exposure on their existing hosting infrastructure. Consciere worked closely with the organization's security group to translate security objectives into a logical infrastructure design with an emphasis on compartmentalization and segmentation of existing and future application environments. After developing a high-level logical architecture, Consciere consultants worked with internal operations and engineering teams to integrate various existing central services into the proposed environment to eliminate redundant and unnecessary service duplication. Consciere is now in the process of supporting deployment of this environment, and helping the organization develop critical technical standards and security policies specific to the high security environment.