Corsec

Opening Markets Through Security Certifications

Capabilities Overview

Corsec

"**Corsec was excellent to work with in getting our Nutanix product line Common Criteria-certified**. We look forward to working with them again on future projects, and highly recommend them to other organizations wanting to get their products certified."

— **John Jensen,**
Director of Engineering Program Management, Nutanix

More than **1 million hours** of **security validation** and **certification consulting** completed.

Relationships with more than **40 testing labs around the world.**

We have the **largest dedicated staff** of engineers in the industry.

We have worked with more than **325 unique** products.

FIXED price, **FIXED** timelines. **Guaranteed.**

We have secured over **350 certifications,** more than any other company in the world.

Tap Into New Revenue and New Markets

Access new markets and secure untapped revenue streams by developing an IT security certification strategy for your products.

With Change Comes Opportunity: Take Advantage of the New IT Security Landscape

The staggering pace of change in technology in recent years has been accompanied by a similarly sharp rise in the number and sophistication of cyber threats. U.S. and international governments have led the charge to protect their critical infrastructures by requiring security certifications for IT products in their procurement processes. Government best practices are also increasingly being followed by private-sector industries, including energy, utilities, health care, and financial services, making certified and validated products highly sought after for many security-sensitive networks around the world.

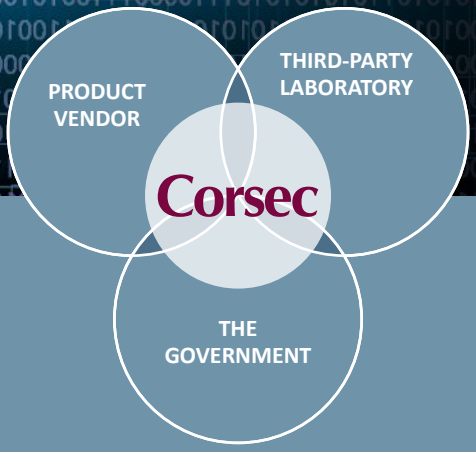
Why Pursue Certifications?

In addition to lucrative financial gains from sales to new markets, security certifications can also confer several other strategic benefits upon a product vendor, including providing assurance to its customers, investors and shareholders that the organization is invested in maintaining the highest levels of product security, and, in turn, mitigating risks to its reputation and brand from potential data breaches.

Perhaps the foremost reason that a product vendor pursues security certifications is to reinforce or gain a competitive advantage against its rivals. It is imperative that an organization know and understand its competitors' security certification status, as this knowledge will arm it with the ability to plan for and achieve certification levels that will leapfrog its rivals from a feature/functionality and security confidence perspective.

"**Corsec did a great job in the planning, guidance and execution throughout the entire FIPS 140-2 process**. Their expertise and prompt response played a tremendous role in the successful completion of our FIPS 140-2 validation."

— **Eric Jen,**
Director of Engineering,
Openpeak, Inc.



The Key Players

Here are the key players in the security certification effort:

The Government

Government entities set mandates for product security policy in their respective countries. They are ultimately responsible for issuing security certifications, stating that product vendors have completed the validation process. They are the regulatory authority focused on standards, rules and policies.

IT Product Vendor

Product vendors wishing to sell into governments or enterprises have to go through third-party security certifications and validations to ensure their products meet the requisite standards for deployment. They must have a conforming product, understand all the key certification requirements, and submit the required documentation to a third-party laboratory for testing. As standards change, they must interpret those changes and translate them into their products.

Third-Party Laboratory

Third-party laboratories are accredited by the government in the country or scheme in which they operate. They play the "testing" role in the process, by verifying that product vendors have documented evidence of adhering to the standards of the certification desired. They are impartial in their assessment and work with the government /scheme until testing is completed.

Certification Consultant

The world of security certifications can be bewilderingly complex. There are numerous certifications which are mandated for different reasons in different markets, have extremely varied processes and procedures, and which can require unique, and sometimes conflicting, product changes. Understanding the intricacies of the certification landscape can be difficult. Product vendors augment their internal capabilities and go-to-market readiness with a consultant, like Corsec, who successfully guides them through the process.

"[Common Criteria] certification is an absolute must for us, as governments world-wide seek to deploy our security solutions. **Corsec came with the highest references from other partners of ours in the security industry**."

— **Throop Wilder,**
Co-Founder & Vice President of Marketing, Crossbeam Systems

Enabling a Successful Certification

Planning

Prior to beginning a certification effort, companies should have a firm grasp of the level of effort, in terms of time, resources and costs, that it takes to successfully complete the process, as well as the expected return on investment. They should understand who the key players are, the benefits, risks and challenges to pursing a certification, how lengthy the process will be, and how much effort and cost it will take to successfully complete. Corsec's Advisory Services can prepare organizations for this complex and lengthy journey.

Product Design Changes

Product design changes are often needed to meet the different requirements of third-party certifications and security validations. These modifications can often be very expensive and require changes and revisions to product road-maps. Corsec's Design Engineering Consulting Services provide guidance on the best and most efficient design for our clients' products.

Documentation Creation & Engineering

Documentation is the cornerstone of the security certification effort. Each security certification has its own unique requirements for documentation that must be written in a highly specialized manner and submitted to the testing laboratory for review. In addition, a complete validation usually includes algorithm testing (FIPS 140-2), test case development (Common Criteria) or STIG Testing (UC APL). Corsec's Documentation Services addresses all documentation creation requirements, while our Engineering Services alleviate the burden of algorithm testing, test case development and STIG testing from our clients' internal teams.

Laboratory Testing

Third-party laboratories perform in-depth testing to ensure a product adheres to the rigorous standards of each security certification. They create a final, detailed report which is sent to the government oversight agency for review and certificate issuance. This stage of the process can last 6-9 months. Corsec's Enterprise Lab Services eliminate the management, headache and risk of mistakes often associated with direct engagement with labs.

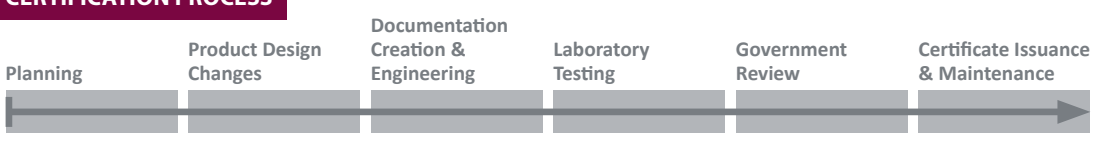
Government Review

The government performs a final review of the laboratory documentation to guarantee the product meets applicable standards, and conducts its own review and testing. This stage of the process can take, on average, 3-6 months.

Certificate Issuance & Maintenance

The complex and lengthy process concludes with the issuance of the security certification. It is important for product vendors to be aware, however, that most security certifications are version-specific; therefore, to ensure continuing benefit from the initial investment, an organization should understand the revalidation or recertification process for the standard in question. Corsec's Maintenance & Compliance Services assess the best path forward for clients, with little to no disruption of their revenue stream.

CERTIFICATION PROCESS



The standard certification process takes 12–14 months.

Certifications Defined

There are three main security certifications that an organization can pursue for its products: **FIPS 140-2**, **Common Criteria**, and the Department of Defense's **Unified Capabilities Approved Products List (UC APL)**. Corsec has separate practice areas for each of these certifications.

FIPS 140-2

With the rising threat of security breaches in today's technology landscape, the need for products that can deliver a high degree of trusted protection has been amplified. The United States' National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE) oversee the **Federal Information Processing Standard 140-2 (FIPS 140-2)** as a standard for systems that process Sensitive But Unclassified (SBU) information to address that need. FIPS 140-2 defines the security requirements for hardware, software, or firmware that use cryptography.

Why attaining FIPS 140-2 validation is valuable

A FIPS 140-2 validation is required before any IT product containing cryptography can be sold to the U.S. Government. This standard has also been adopted in the financial services, critical infrastructure and healthcare industries, and by governments in Europe, Latin America and Asia.

Because FIPS 140-2 is a comprehensive requirement set for cryptographic modules that is recognized and respected across the globe, attaining FIPS validations gives a company significant competitive advantages for your products.

Common Criteria

Common Criteria is an internationally recognized set of guidelines for information technology security products. It provides assurance to buyers that the process of specification, implementation, and evaluation for any certified computer security product was conducted in a thorough and standard manner. As of September 2014, twenty-seven countries have signed the Common Criteria Recognition Agreement (CCRA), making the certification a standard that translates globally and provides an unparalleled measure of security for the international commerce of IT products.

Why pursing Common Criteria certification is important

A Common Criteria evaluation provides an independent review and analysis of a product's or system's security against an Evaluation Assurance Level (EAL) and/or against a defined set of requirements (Protection Profile) for that product or system type.

This certification represents a level of product security and commitment that is required for access to U.S. and international government markets, but can also serve as a competitive differentiator when marketing to non-government clients in other industries, such as financial services/banking or healthcare.

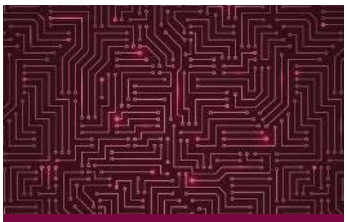
Unified Capabilities Approved Products List (UC APL)

The U.S. Department of Defense created the **Unified Capabilities Approved Products List (UC APL)** in 2011 to identify solutions that can be trusted to address its security concerns. DoD agencies looking to build their technology infrastructure may only purchase products from this list, giving vendors on the UC APL a competitive advantage. Along with this lucrative revenue opportunity, this list acts as a stamp of approval to many corporate procurement teams, opening the door to even more potential revenue.

Getting listed on the UC APL

To be included on the UC APL, products must complete a 39-step process overseen by the Unified Capabilities Certification Office (UCCO). The process includes the submission of properly-completed forms and product documentation, attainment of prerequisite validations and certifications such as FIPS 140-2 and Common Criteria, and adherence to strict scheduling guidelines and interdependencies. The specific requirements for a given product depend on its security category and are defined in the UC APL's Security Technical Information Guides (STIGs). Products also must pass Information Assurance (IA) and Interoperability (IO) tests conducted at one of the DoD's Testing Centers of Excellence. These tests are intended to ensure that a product meets the required level of security and integrates into an existing infrastructure without introducing operational risk.

Corsec's Solution Offerings for Federal Certifications and Security Validation



FIPS 140-2

Satisfies

U.S. (NIST), Canada (CSEC), Commercial, and Cryptographic Requirements

Fits Into

COMMON CRITERIA

Satisfies

U.S., Civilian, Enterprise, 27 Member Countries, and Supply Chain Requirements

Fits Into

UC APL

Satisfies

DOD/DISA Requirements

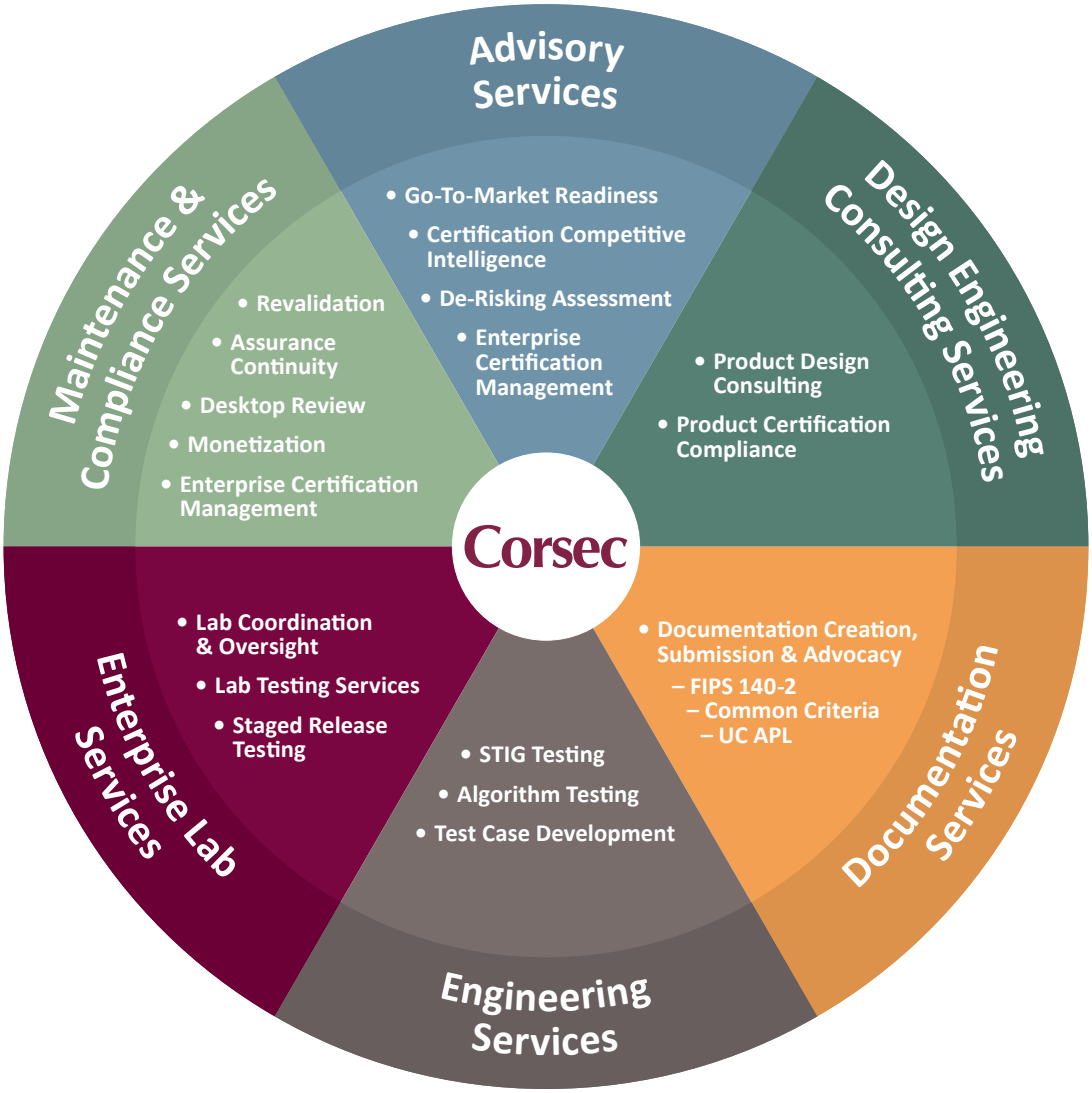
Fits Into

CORSEC'S ENTERPRISE CERTIFICATION STRATEGY FOR:

Cryptography Requirements, Supply Chain Validation, U.S. Federal (Civilian), U.S. Federal (Defense), U.S. Federal (NSA/Classified), Global Enterprise & Commercial, 27 Member Countries

The Corsec Solution

Corsec's guidance through the maze of certification processes can be the difference between generating revenue when it was budgeted and having to delay and reforecast, perhaps for months or even years.



Our offerings are categorized into six service areas:

Advisory

Making the decision to seek a product security certification is not one an organization should enter into lightly. Prior to beginning the process, companies must be well-versed in the many details involved, and have a firm grasp of the level of effort, in terms of time, resources and costs, that it takes to successfully complete the exercise, as well as the expected return on investment. Corsec's **Advisory Services** offerings are designed to equip organizations with the information they need to successfully achieve the certification they are seeking.

Design Engineering Consulting

Product design changes are often needed to meet the different requirements of third-party certifications and security validations. Corsec's **Design Engineering Consulting Services** are complementary to our Documentation Services and provide guidance on the best and most efficient design for our clients' products, to enable them to move swiftly through the certification process.

Documentation

Corsec's **Documentation Services** are the cornerstone of the certification effort. They encompass documentation creation and submission, as well as clarification, defense and advocacy. All of these are completed within a system of assured quality that includes client engagement, Corsec's peer-to-peer global quality panel review, and issue advocacy with the lab and the scheme.

Engineering

A complete validation usually includes algorithm testing and implementation (FIPS 140-2), test case development (Common Criteria) and STIG Testing (UC APL). These services are beyond the traditional domain of documentation and certification consulting. Historically, most companies have chosen to perform these tasks themselves, not realizing the totality of the burden and cost on their organizations. Corsec's **Engineering Services** will relieve this load from internal teams so they can remain focused on revenue-generating activities.

Enterprise Lab

Corsec's **Enterprise Lab Services** are government- and scheme-agnostic, and offers customers access to a host of vetted labs globally through the Corsec Lab Provider Network. These services enable Corsec to assist product vendors with selecting the appropriate Scheme/country where their product should be evaluated, matching customer requirements (ITAR, etc.) with laboratories suitable to handle that requirement, and helping customers understand the pros and cons of different options, and providing a path forward.

Maintenance & Compliance

Technology is ever changing and a product that has been certified or validated will likely need to go through the process again. Corsec's **Maintenance & Compliance Services** can help determine whether a full reevaluation is necessary, or if companies can pursue other measures to continue generating revenue from their initial certification or validation.

Solution Bundles to Fit Your Needs

Pulling from each of our service areas, we have created a range of service bundles for each of the certifications we support, to address the varying requirements of our customers. **Each bundle type targets clients with different needs, by building on itself to form the next level of offerings:**

Core Solution

For those companies who are seeking guidance with a limited scope of services, our **Core Solution** pulls from our Advisory, Design Engineering Consulting and Documentation Service areas, and covers certification fundamentals, including a De-Risking Assessment, Product Design Consulting and Documentation Creation.

Enhanced Solution

In addition to the documentation set, all key certifications require additional engineering efforts. With FIPS 140-2, the requirement is Algorithm Testing. For Common Criteria, it is Test Case Development. And, for UC APL, the requirements are STIG testing and the SAR. Corsec's **Enhanced Solution** augments vendors' engineering capabilities by completing these requirements.

Turnkey Solution

For companies seeking the least risky path to certificate issuance, or companies with critical go-to-market timelines, the **Turnkey Solution** is designed to cover every possible need. It includes the Enhanced Solution, plus all phases of lab testing, all government fees, and program management and oversight. It is a solution for companies requiring end-to-end management of the certification process.

"ScienceLogic now holds the distinction of being the first-ever complete end-to-end IT infrastructure monitoring company named to the DoD's UC APL. **The guidance we received through our partnership with Corsec proved critical in our success.** Achieving this critical milestone is a massive achievement that opens the door to the DoD and beyond."

— **Dave Link,**
Co-Founder and CEO, ScienceLogic

FIPS 140-2

Satisfies Cryptographic Requirements for U.S. / International Government and Commercial Markets

CORE SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services		
ENHANCED SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• Algorithm Testing • Lab Oversight & Monitoring • Project Management	
TURNKEY SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• Algorithm Testing • Lab Oversight & Monitoring • Project Management	• Lab Testing Services • Staged Release Testing • Enterprise Certification Management • Certification Maintenance

Common Criteria

Satisfies Information Assurance and Supply Chain Requirements for U.S. / International Government and Commercial Markets

CORE SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services		
ENHANCED SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• Test Case Development • Lab Oversight & Monitoring • Project Management	
TURNKEY SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• Test Case Development • Lab Oversight & Monitoring • Project Management	• Lab Testing Services • Staged Release Testing • Enterprise Certification Management • Certification Maintenance

Unified Capabilities Approved Products List (UC APL)

Satisfies DoD / DISA Requirements

CORE SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services		
ENHANCED SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• STIG Testing • TCOE Oversight & Monitoring • Sponsor Coordination • Project Management	
TURNKEY SOLUTION	• De-Risking Assessment • Product Design Consulting • Documentation Services	• STIG Testing • TCOE Oversight & Monitoring • Sponsor Coordination • Project Management	• Desktop Review • TCOE Coordination

Custom Services for a Complete Solution

Corsec's expert services address the needs, challenges, and potential roadblocks encountered by clients in many certifications and validations.

Enterprise Certification Management

Corsec's **Enterprise Certification Management Services** provide strategic planning guidance that allow leadership to stay on top of the overall strategic issues of certification without getting too deeply immersed in the often-overwhelming details.

Product Design Consulting

During the security certification process, product design changes may be necessary to meet validation requirements. Corsec's **Product Design Consulting Service** helps clients devise the best and most efficient way to create or modify a design in order to obtain certification.

De-Risking Assessment

The **De-Risking Assessment** offers key members of a client's team a look at the critical aspects of any certification process, covers requirements, describes any points that could become obstacles, and provides an opportunity to ask questions of Corsec staff.

Documentation Services

Certification documentation is complex and can pull companies away from revenue-generating projects. Corsec's **Documentation Services** leverage the experience of the largest team of experts in the industry to streamline documentation and remove this burden from our clients.

"We started the process almost two years ago with a very limited understanding of the FIPS 140-2 certification process. **With their proven expertise in this field, Corsec helped get us realigned in the right direction and has kept us on track throughout the process**, allowing us to complete the certification with no surprises."

— **Vivek Gupta,**
Sr. Director, Software Engineering,
Hughes Network Systems

Algorithm Testing

Passing **Algorithm Testing** is one of the most critical and challenging steps of the FIPS 140-2 validation process. Corsec's experience helps clients avoid pitfalls, and our patent-pending tool, **Ultima**, streamlines the process even further.

Test Case Development

Test Case Development and testing can be cumbersome, especially during the critical phase of the Common Criteria effort. It invariably ties up the engineering and QA teams for months. Corsec's **Test Case Development Service** can ease the burden, ensuring that the certification stays on track, and the QA department is not derailed.

STIG Testing

Listing products on the DoD's Unified Capabilities Approved Products List (UC APL) is lengthy and complex, and includes mandatory STIG testing. Our **STIG Testing Service** can manage the testing portion of this process, and even shorten this phase of the evaluation.

Lab Testing Services

Our **Lab Testing Services** offer customers access to a host of vetted labs globally, as well as the experience of a dedicated team which guides them through lab selection and testing, streamlining the path to market.

Staged Release Testing

Reduce the risk of failing the testing process with Corsec's **Staged Release Testing Service**. This service enables results to be provided earlier in the development cycle, allowing more time to react to and correct any deficiencies identified.

Go-to-Market Acceleration

Corsec's **Go-to-Market Acceleration Service** is designed to give companies a jump-start immediately upon receiving their certification, so that no time—or revenue—is lost on confusion about how to properly market or sell their new certification.

Certification Maintenance

A product that has been certified or validated will likely need to go through the process again. Corsec's **Certification Maintenance Service** helps customers determine whether a full recertification is necessary, or if there are other options that may be less costly and time consuming, as well as guides them through the process.

Corsec

Opening Markets Through Security Certifications

Security Validation Consulting and Solutions

Corsec is a boutique security engineering firm that serves as a guide for companies looking to access new markets through validation and certification of information technology products. Like other security certification consultants, Corsec offers its customers assistance in creating the extensive documentation required during these processes. However, unlike the competition, Corsec goes beyond the basics, to provide an overarching view on IT security validation, giving consultation on business issues, product lifecycles, development timelines, and the overall financial considerations associated with certification strategy and achievement.

Our team comes with **more than 100 years of proven techniques, processes and applied methods** in security validation and certification consulting.

Extensive Industry & Technology Expertise

Having worked as engineers in a FIPS testing laboratory, and having seen first-hand the difficulty that product vendors experienced as they progressed through the certification process, Corsec's founders recognized the need for an organization to act as a guide for companies through this maze. In 1998, they founded Corsec, the "core of Corporate Security," with a singular mission of enabling security validations and third-party certifications through a system of assured quality, advocating for the product vendor, and providing a system of checks and quality controls and a process for assuring validation will occur on time and within budget.

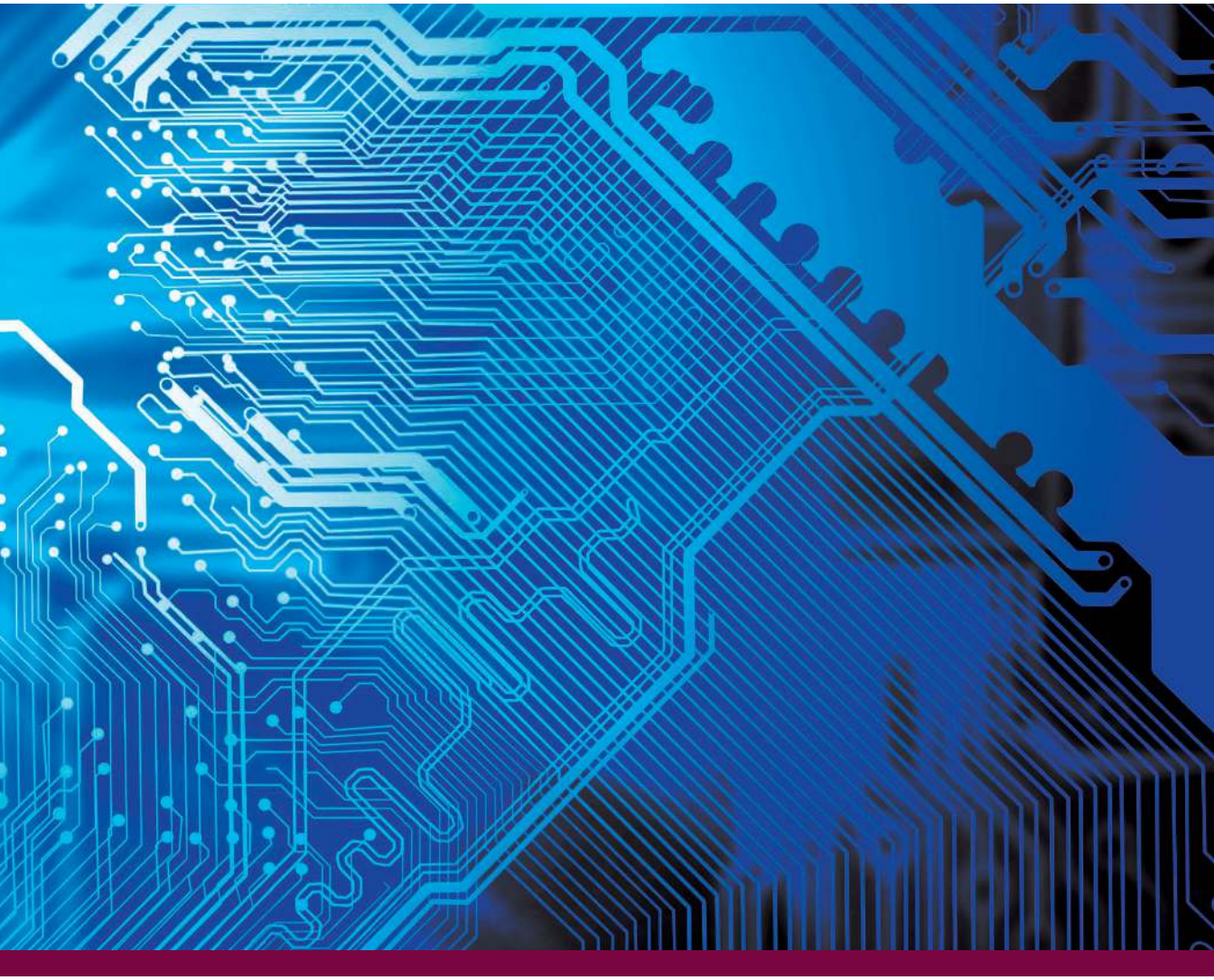
With over 100 cumulative years of experience and the largest dedicated staff of experts in the industry, Corsec has secured more than 350 certifications for hundreds of organizations, from start-ups to Fortune 50 companies, on five continents – more than any other company in the world. Our familiarity with the newest technologies, experience with a vast number of device types, solid relationships with testing laboratories around the world, and our collaborative Quality Review Panel, which ensures that our clients benefit from our diversity of experience and leverage our collective brain trust, gives our customers an advantage that allows them quicker access to new revenue streams.

Create a roadmap for future security certification and validation with Corsec as your guide.

Corsec

"Caymas is delighted to have worked with Corsec's exceptional staff on quickly and efficiently achieving FIPS 140-2 validation. **The high quality of work produced paired with their resourceful project management positively reflects upon the expertise of the company.**"

— **Sridhar Venkatesh,**
Director of Product Line Management,
Caymas Systems



/// CORSEC.COM

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
703.267.6050
info@corsec.com

Corsec