INFORMATION SECURITY

SAFEGUARDING YOUR SYSTEMS AND PROTECTING YOUR ASSETS

Security is an integral part of all our customer engagements, and our cybersecurity team keeps it top of mind regardless of project size. We optimize your approach to information security—based on expertise, industry best practices, and an eye towards embracing Digital Innovation.

Our certified security specialists stay current with the latest techniques and technologies to provide the guidance, processes, and services needed to safeguard data and protect your assets. We know the ins and outs of complex industry regulations and can provide the support you need to ensure compliance and get your products to market on time.

BASE2 ADVANTAGES

Cybersecurity frameworks. Our highly experienced security experts help your organization choose and tailor the right cybersecurity framework to address your security concerns or meet regulatory compliance.

Auditing and remediation. The first step in implementing a cybersecurity framework is establishing a baseline. We start with an audit against a cybersecurity framework and provide you with a gap analysis. Once a baseline is established, our staff can assist at any level needed to help your company remediate missing requirements, bringing you into compliance.

Penetration testing. Your ability to ward off a breach and demonstrate continued cybersecurity compliance is paramount. Our security team can provide a detailed penetration test on any level your company needs and make recommendations to remediate all findings.

Device and code testing. Our team performs device and application testing to ensure your product is secure and ready for production. Leveraging industry best practices and tools, we provide white or black box testing and can assist with remediation based on findings.

We recommend embedding a security engineer within all projects to ensure that security issues are addressed from project implementation. This helps projects avoid delivery delays or costly code rewrites associated with finding vulnerabilities later in the software delivery life cycle.

CUSTOMER SUCCESSES

From ensuring the security of patient data to comprehensive security audits, our experts have helped clients understand and remediate vulnerabilities.

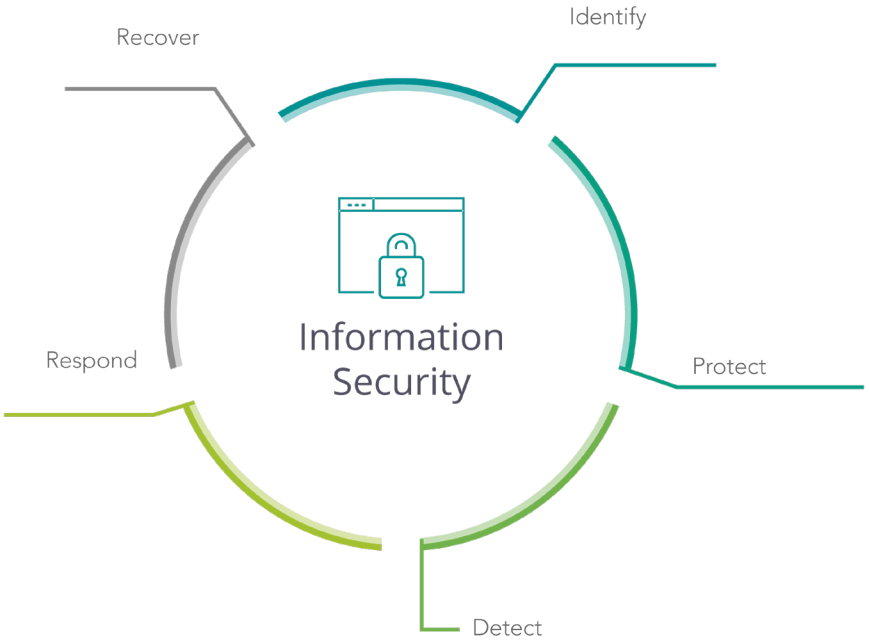
> Completed a rigorous HIPAA compliance assessment for a healthcare provider in just six weeks. Our team evaluated employees, IT systems, hardware, software, patient access procedures, and patient record storage and created a remediation action plan that enabled the provider to achieve HIPAA compliance in just two months.

> Performed a detailed security audit by examining voluminous amounts of documentation relating to a product slated for a commercial aircraft, developed and performed physical test procedures from the resulting analysis, and authored a findings documents with security recommendations that allowed the client to remediate the issues our experts found.

WHERE WE CAN HELP

Most information security frameworks share similar functions that should be performed on a concurrent, continuous basis. Our security experts lend their expertise from end to end, or anywhere in between.

- Identify the parameters of managing security risk to systems, people, assets, data, and capabilities, from the business environment to asset and risk management
- Establish the processes, technologies, and systems to effectively protect data, assets, and networks
- Detect anomalies, events, and other threats and implement continuous monitoring
- Take action when a threat is detected, from response planning and communication to mitigation and program improvements
- Develop and implement plans for responding to a security incident and rapidly restoring capabilities and services.



FRAMEWORKS & STANDARDS

NIST 800 Series

CIS

GDPR

PCI-DSS

HIPAA

ISO 27001/27002

OWASP

SECURITY CERTIFICATIONS

CISSP

CSSLP

GPEN

GWAPT