



## End-to-End Information Security You Can Trust

Your business and mission depend on the information and assets you are entrusted to protect

Information security is only as strong as its weakest link. ABS.C's complete lifecycle information security solutions:

- Reduce exposure before you deploy by applying the right team to identify and address threats before they jeopardize your assets
- Save money and time by discovering security threats early in the development lifecycle using a risk-based approach
- Minimize calamity after a breach with rapid response and mitigation

## Information Security That Prevents, Protects, Assesses, and Resolves

Holistic information security services during all phases of the development lifecycle

### **Architectural Risk Analysis:** identify and mitigate flaws in system architecture

Identification of flaws in the software architecture alerts you of risk to business information assets that may result from those flaws early in the development process.

### **Secure Code Review:** assess the security and quality of code as it is developed

Integration of secure code review throughout the stages of the system development lifecycle yields dramatic results to the overall quality of the code, allowing you to address risks proactively rather than after an incident.

### **Incident Response:** minimize the impact of a security breach

Identifying a breach, assessing what was compromised, and putting a mitigation plan in place minimizes impact to your information, assets, and your mission or business.

### **Application Security Testing:** reveal vulnerabilities before they expose you to risk

Analyzing the security of your system during development reveals potentially hidden or embedded flaws that may put your entire enterprise at risk.

### **Penetration Testing:** identify and mitigate potential vulnerabilities to your enterprise

Simulating an attack on a computer system or network assesses potential vulnerabilities that could result from faulty system architecture, exposure from COTS products, hardware and software flaws, and operational weaknesses.

### **Network and Computer Forensics:** discover the source of security attacks

Capturing, recording, and analyzing network and computer events is vital to discovering the source of security attacks or other incidents, equipping you with valuable knowledge that translates into even better security.

### **Malware Analysis:** know what is attacking your system

Identifying and analyzing viruses, worms, Trojans, adware, spyware, backdoors, and rootkits is important in order to understand the impact they may have had on your system or network.

## Why ABS.C?

Proven performance. Trusted by the Intelligence Community. Best practices of the Private Sector.

We care about the information your business and mission depends on. Maybe it's our proven track record of supporting Intelligence agencies by helping them protect their most sensitive information. Or perhaps it's the work ethic of our people who tirelessly support our clients. Whatever the reason, ABS.C is the right partner when it comes to information and hardware security.

**Holistic support** – our trusted team of experts work collaboratively throughout the development lifecycle to deliver integrated support

**Proven performance** – the results we deliver exceed client expectations

**Cleared professionals** – All of our security experts hold security clearances