

## THE IGP AND CFSR: TRANSITIONING YOUR E-DISCOVERY CAREER INTO A CYBERSECURITY ONE

The second part of this look at cybersecurity education and certifications explores two certifications that touch on both cybersecurity and e-discovery: the IGP and CFSR.

BY JARED COSEGLIA

Part one of this series, “**Maneuvering the Madness of Cyber and ESI Education & Certification**,” examined some basic and broadly accepted industry-standard certifications that can be achieved within a year’s time or less: CEDS (Certified E-Discovery Specialist), GIAC (Global Information Assurance Certification) and RCA (Relativity Certified Administrator) programs. CEDS and RCA are distinctly e-discovery, one vocational (product-specific) and one educational. GIAC is squarely focused on cybersecurity.

Part two, meanwhile, aims to expose two lesser-known but rapidly accepted certifications, the IGP (Information Governance Professional) from ARMA International (Association of Records Managers and Administrators) and the CFSR (Certified Forensic Security Respond-

er) from Guidance Software Inc., makers of EnCase and the EnCE. Both certifications aim to aid e-discovery and cybersecurity professionals alike, but in very different ways.

From a reference model perspective, e-discovery (EDRM) and cybersecurity (CSRM) overlap in two core areas: forensic investigation/incident response and information governance. The EDRM moves from left to right taking data from volume to relevance. The CSRM moves from left to right taking a security approach from proactive to reactive.

When comparing job responsibilities along the EDRM with the CSRM, we find forensic collection is far left in EDRM (volume) but far right in CSRM (reactive), creating an immediate and applicable overlap between cybersecurity incident



JARED COSEGLIA

responder and discovery forensic collection and investigation skill sets. This intersection is where forensic professionals in e-discovery should look to transition their career to cybersecurity, following the trend that demand is slowly decreasing for forensic collections in discovery while widening and growing in incident response.

## The Certified Forensic Security Responder Certification

The Certified Forensic Security Responder certification program, created and administered by Guidance Software, is specifically designed to help forensic investigators transition to cybersecurity and incident response. Guidance is best known for EnCase and its certification, the EnCE. Guidance, specifically EnCase, has been considered a market leader in proprietary forensic technology for collection and investigation for over a decade. This year's Enfuse conference, an event like Relativity Fest, clearly indicated the company's firm shift ("Don't Fear the Breach" T-shirts) toward cybersecurity products and services leveraging their existing technology as a platform for the future.

Manfred Hatzesberger, training director and master instructor for Guidance, elaborated on the company's pivot: "We recognized the EnCE was very law enforcement focused, designed to create proper reporting when testifying—particularly in the United States. The global demand for people to move from forensic investigation to incident response was the genesis of the CFSR, which



Credit: SimpleB/Shutterstock.com

is a great first step, especially if you are looking to move into the corporate world."

Much like at Guidance, talent in the federal and government sectors are aggressively matriculating toward the cybersecurity private sector. Many of these professionals have been using EnCase for years. Hatzesberger echoes the foundational need for EnCase across both disciplines, "When one performs a breach remediation, incident response or other hacking-related cyber task, at some point in their process they need to find the artifacts in a way which requires forensic tools and experience. The EnCE is geared toward forensics, but it is the basis for everything," Hatzesberger explained.

So, the CFSR may not be your starting point if you are not already EnCE certified. "It helps if

people pursuing the CFSR use EnCase and Guidance products on a regular basis. If you have not used EnCase products, the certification program becomes more complicated," said Hatzesberger.

The CFSR is very new. So far there are just over 50 individuals certified and counting. Meanwhile, Guidance maintains an estimated 6,000+ people with an EnCE. The CFSR is valid for three years and requires a 32 CPE accreditation and/or one year of applicable work experience in incident response and passing the exam, which can be administered at the annual Guidance Enfuse conference held in the spring of each year. Courses are also offered throughout the year regionally.

The CFSR is very hands-on, using not only Guidance products but a wealth of open

source technology. This is a product-specific cert; however, according to Hatzesberger, the training courses for the CFSR are “very open-minded about and incorporate other products in the market used in the field.” Still, the CFSR should be viewed as a vocational certification, much like the RCA, rather than a broad educational certification, like the IGP.

### **The Information Governance Professional Certification**

The Information Governance Professional certification is a non-tool-specific validation of the knowledge necessary to help an organization leverage information for maximum value while reducing the costs and mitigating risk. For e-discovery professionals, the IGP is aimed at people who are invested in bringing volume to relevance by reducing data sets early in the information life cycle. For cybersecurity professionals, the IGP aids them in being conversant with principles, risks and tasks around security in the context of information governance.

Notably, the IGP credential integrates all eight of ARMA’s **Generally Accepted Record-keeping Principles** into an overall framework for effective information governance. Two of

these principles are particularly relevant to cybersecurity professionals: integrity and protection.

Diane K. Carlisle, information governance program advisor for ARMA and IGP, said the target audience for IGP is “anybody who aspires to be in upper management making key decisions related to managing information assets as a critical component of moving the organization forward.” This certainly applies to professionals in both e-discovery and cybersecurity. In many ways, the IGP can bridge the gap between these two disciplines.

“Legal and IT often have different goals for the organization, and sometimes those goals contradict one another,” added Carlisle. “Balancing these competing needs in terms of managing the information as well as optimizing the organization as a whole is a core goal of the IGP certification.”

While the IGP—like CEDS for ESI in many ways—is a broader educational foundation for information governance professionals, it is still working to gain greater visibility and universal acceptance among client bases. There are 300-plus accredited IGP professionals in the United

States. An IGP certification is valid for three years, and ARMA just went through its first IGP “recertification” since its inception in 2013. The backgrounds vary for professionals with the certification from practicing attorneys, legal department managers and corporate counsel to a wealth of independent consultants and practitioners. The IGP serves as a strong differentiator if you are a consultant in the space. Applications get turned around very fast, and applicants must test within one year of application approval.

ARMA has a published list of suggested resources to prepare to take the IGP and has a study guide for sale that includes a self-assessment tool. Some ARMA chapters have self-organized into study groups, but no formal training program exists currently from an institutional standpoint. Like Guidance, ARMA has an annual conference where it teaches a half-day preconference session that goes over the content of what’s covered in the IGP exam.

Stay tuned for part three of “Maneuvering the Madness,” where we will explore additional certifications in the ESI and cyber industries!