

Unified Management System (UFMS) Case Study

Agency: Department of Justice (DOJ)

Business Integra worked with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, that provided guidelines to federal agencies conducting security Certification and Accreditation (C&A) of information systems.

We worked with DOJ IT Security Standards that are divided into the three security control categories used by NIST: management, operational, and technical controls. Our in-depth knowledge about Certification & Accreditation process that does the full assessment of an information system's security controls (including management, operational, and technical security controls) enabled us to determine how well they are implemented.

Business Integra worked on the goal of certification testing to determine whether the security controls that have been identified for the programs such as UFMS in the System Security Plan (SSP) are effective in supporting the minimal security requirements under NIST SP 800-53 Revision 1, Recommended Security Controls for Federal Information Systems. We worked on Systems development, deployment, and operations that are guided by a hierarchical set of policies. Federal laws, regulations, and executive mandates, along with high level DOJ policies, that provided the overarching basis for many of the lower level standards and policies. The hierarchy of DOJ IT Security policies and standards are:

Overarching Edict	List
Federal laws, regulations, and executive mandates	Federal Information Security Management Act (FISMA), Federal Information System Controls Audit Manual (FISCAM), Continuity of Operations (COOP), Cyber Security Assessment and Management (CSAM), Computer Environment and Enclave Defense (CEED), Federal Information Processing Standard (FIPS), U.S. Section 552a - the Privacy Act, Public Law 100-235 - The Computer Security Act, National Institute of Standards Technology (NIST), 28 Code of Federal Regulations (CFR) Part 17, 32 CFR Part 200, DCID 6/3, 6/4, 6/9
Department level	DOJ 2640.2e, DOJ 2630.3a, Executive Order (EO) 12958 - as amended, EO 12968, Technical Reference Manual (TRM), and Security Program Operating Manual (SPOM)

We architected and published the DOJ UFMS Security Architecture document that described how the system is in compliance with DOJ IT Security Standards. Within UFMS, the various mechanisms required to protect UFMS information from vulnerability across physical, network, operating system, application and database communication layers have been implemented. The appropriate procedures were enabled to secure end-to-end communication between UFMS end user/client desktop, middleware web and application servers and backend information storage servers that are within the scope of UFMS architecture design. The UFMS, where feasible, has enhanced the minimum security requirements in compliance with DOJ IT Security Standards to support secure transactions of UFMS business, delivery of information between department, Components and other federal, state and UFMS business trading partner companies.

We have designed and delivered many highly visible and mission critical enterprise applications that deal with corporation sensitive, classified and secret data. Our recent DOJ UFMS security architecture design encompasses implementation of security across the following layers to help ensure "defense in depth" or the confidentiality, integrity, and availability of financial information.

START TODAY

In today's market as the companies are relentlessly pushing to compete better, move faster and fight harder, Business Integra Inc is the global solution provider with a single-minded passion: dedicating our systems expertise, industry intelligence and global resources to make your business stronger.

For more information on how Business Integra can improve your presence on the web, contact us at hr@businessintegra.com or visit our website at www.businessintegra.com.