



**EAMMUNE**

## **FEDERAL INFORMATION SECURITY MANAGEMENT ACT (2002)**

### **DRIVING THE NEED FOR AUTOMATED CONTROLS**

**A White Paper for Triumfant**



The Federal Information Security Management Act (FISMA) was created in response to increased awareness at the federal government of risks of cyber-terrorism, and of cyber-security in general. Following in the wake of private sector corporate scandals, FISMA emerged from a similar principle that led to Sarbanes-Oxley Act (SOX) of 2002, unambiguous personal acceptance of risk by a senior management official. In recent years, FISMA has played a crucial role in driving federal agencies to improve their overall security posture, providing a framework and guidance for such efforts. Therefore, compliance with FISMA is critical to keeping agency officials out of legal trouble.

Since federal agencies handle massive quantities of sensitive data – including health records, social security numbers and financial data for the entire citizen population of the United States – they are exposed to heightened attention from cyber-thieves and cyber-terrorists. The potential for disruption of general U.S. government operations by compromising Agency’s computer systems can be of high value to any group that might be seeking to sow confusion. Lastly, these agencies present an attractive target from a public relations perspective for any anti-U.S. terrorist group.

FISMA mandates that all agencies take responsibility for the security of their computer systems. FISMA is a wide-ranging Act that covers all data systems, from servers to desktops, laptops and other personal computing devices, as well as the associated network infrastructure. Agency Computer Information Security Officers (CISO’s) and their subordinates are not only liable for the welfare of their agencies with respect to FISMA, but may also be personally liable for compliance failure in the case of a breach. Even federal government contractors are potentially liable under FISMA.<sup>1</sup>

While FISMA and related federal acts are deemed necessary to protect the citizens of the United States, they have also placed an enormous burden on the agencies, in terms of time, paperwork, and financial burden, particularly on their IT staff. Federal agencies are graded each year on satisfying and meeting these requirements.

As is usually the case with data security driven regulations, in the end what matters is their actual effectiveness, not the regulations themselves. Even with the additional budget and hours dedicated to computer security under FISMA, there is criticism that it has been ineffective and merely just a generator of additional paperwork.<sup>2</sup> Clearly, federal agencies must rely on guidance from FISMA while adopting cost-effective solutions to simplify and automate as much of their compliance initiatives as possible.

---

<sup>1</sup> Joseph, Conn, “Giving Vendors the Bill: Law makes VA contractors liable in security breaches,” *Modern Healthcare*, January 1, 2007.

<sup>2</sup> “INPUT Says FISMA Fails to Improve Overall Security,” *PR Newswire*, March 16, 2006.

## **WHAT IS FISMA AND THE EFFECT ON ORGANIZATIONAL RESOURCES**

FISMA was intended to increase the attention of the federal government agencies to cyber-security, an area that had previously been neglected. FISMA requires that each federal agency “develop, document, and implement an agency-wide information security program ... to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”

FIPS-199 (Federal Information Processing Standard), signed by the Secretary of Commerce in 2003, requires that federal systems be classified in accordance to a defined process into one of three levels of importance to each agency’s operations. This implies that systems are understood comprehensively, that classification boundaries are well-defined, and that all stakeholders agree on classifications, including those with budget authority.

FIPS-200 (2006) defines in specific terms the minimum level of controls necessary to constitute due diligence towards the protection of government assets. Failure to implement or provide adequate assurance of these controls could constitute negligence. FISMA compliance is manifested in the act of system certification and accreditation. The former, certification, usually requires an independent third party to evaluate the existence and effectiveness of controls. The latter, accreditation, constitutes of reviewing the results of certification and the drafting of plans to close identified gaps based on a risk assessment. Lastly, system authorization is the act of formal risk acceptance by an Agency’s officials.

Note that FISMA does not focus on a particular data type (such as financial data), nor only on confidentiality of data. Rather, all data types must be evaluated for all their protection profiles, including: confidentiality, integrity and availability, as they relate to the successful operations of each agency.

### **Mandates and Guidance on Cybersecurity**

The key initiatives and efforts within the federal government's efforts to combat cyberterrorism and enhance computer security include FISMA, the series 800 initiatives by National Institute of Standards and Technology, and Security Content Automatic Protocol (SCAP) and Federal Desktop Core Configuration (FDCC).

**FISMA (2002).** The Act was meant to bolster computer and network security within the federal agencies and affiliated parties (*e.g.*, government contractors) by providing guidance and

mandating regular audits. FISMA requires that each federal agency prove that access to data is tightly controlled and highly secure.

**NIST (Special Publications 800 Series).** One of the requirements of the FISMA legislation is that Federal agency systems must be compliant with minimally accepted system configuration requirements. NIST Special Publication 800-68 was created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional SP2 systems. By implementing SP 800-68's recommendations, its security templates, and its other general prescriptive recommendations, organizations should be able to meeting the baseline configuration requirements for Windows XP systems. Similarly, another NIST special publication, SP 800-53, is made mandatory for all federal systems owners by virtue of FIPS-200, requires a foundational level of security for all federal information and information systems.

**Security Content Automatic Protocol (SCAP).** SCAP is a method for using specific standards to enable automated vulnerability management, measurement, and policy evaluation (*e.g.*, FISMA Compliance).

**Federal Desktop Core Configuration (FDCC).** The FDCC is an Office of Management and Budget mandate and requires that all federal agencies standardize the configuration of approximately 300 settings on all Windows based computers.

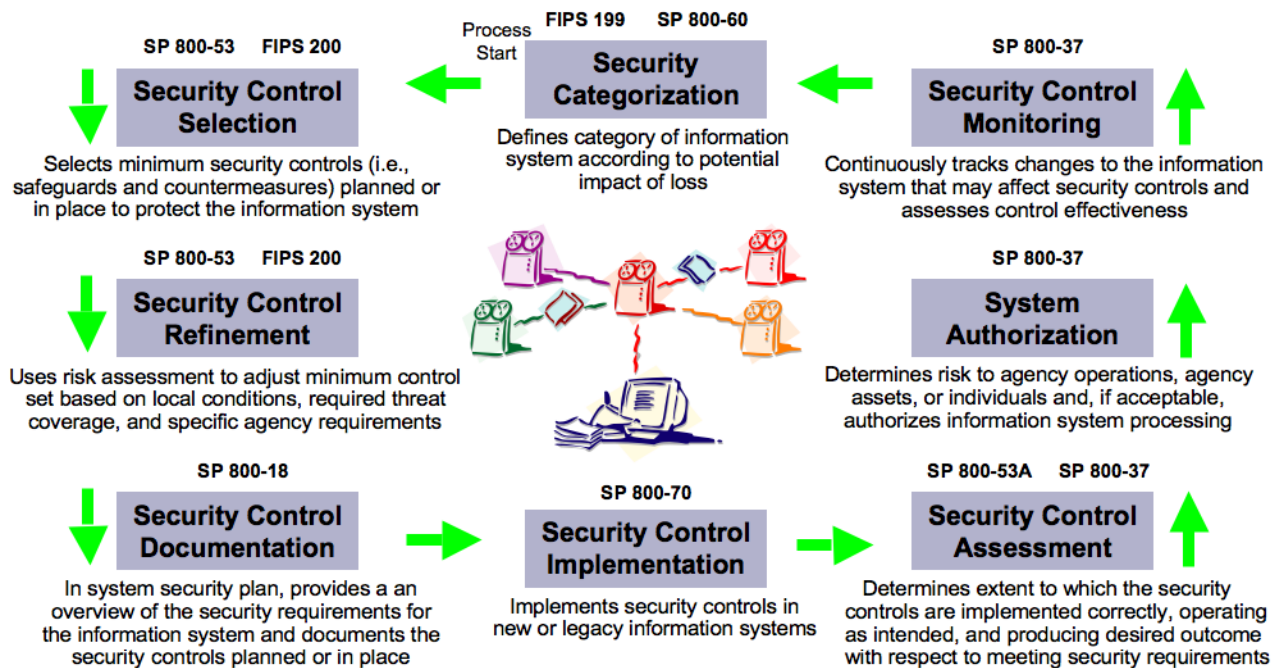
**State Government Legislation.** In addition, governors across the country are issuing Executive Orders for strengthening state information technology security, along the lines of the federal government. For example, as of March 2008, the Governor of Georgia is requiring the Georgia Technology Authority (GTA) to work with the State's Department of Audits and Accounts and the Governor's Office of Planning and Budget to develop a reporting format and required content for agency information security reports. Each agency will be responsible for reporting to GTA at the end of the fiscal year. GTA's Office of Information Security is developing technical security standards and services for use by all of the state's agencies, consistent with the information security risk management model produced by NIST in support of FISMA.<sup>3</sup>

In fact, some requirements in NIST publications make system owners accountable to the information security practices of third parties involved in handling agency data. This has resulted in a "trickle down" effect, as state, regional, local and tribal entities, as well as private contractors, realize

---

<sup>3</sup> Gov. Perdue Signs Executive Order Strengthening State's Information Technology Security, *US Fed News Service*, including *US State News*, March 19, 2008.

the importance of being able to express assurance in a way that is acceptable and communicable to their partnering agencies. The NIST management framework can be depicted as follows:



### Examples of Federal Government Breaches and State of Vulnerability

There are many examples of computer security breaches in the federal, as well as state government agencies. Many federal agencies have been breached multiple number of times, and in various ways. This has prompted many different Committees in the House of Representatives and the Senate to call the senior management of various federal agencies in for hearings.

**Department of Veteran Affairs.** The VA has had multiple and significant breaches. In May 2006, a computer holding 26 million records was stolen from a VA employee's home. The veteran's health and information Act took effect immediately in December, 2006 which holds the VA and their vendors liable.

**Department of Agriculture.** The Department of Agriculture maintained a website that made the social security numbers of those who received aid, as many as 38,700 people, were publicly available before they were taken down in April, 2007. Second, in June 2006, the Department of Agriculture reported that a hacker broke into the Agriculture Department's computer system and may have obtained names, Social Security numbers and photos of 26,000 Washington-area employees and contractors, the department said. Secretary Mike Johanns indicated that the Department will provide free credit

monitoring to anyone affected for the period of one year<sup>4</sup>

**Federal Emergency Management Agency.** In April 2007, the *Washington Post* reported that FEMA printed the social security numbers of 2,300 people on the outside of their Disaster Assistance Employee reappointment letters after Hurricane Katrina.

**Internal Revenue Service.** In April 2008, the Treasury Department's own watchdogs reported that the IRS was extremely vulnerable and that a disgruntled employee or a hacker could gain access to the IRS's entire network.<sup>5</sup>

## **FISMA, OTHER LEGISLATION AND THEIR IMPACT**

Legislations and the need to protect the government's information assets have placed tremendous pressures on each Agency's CISO and their staff.

### **Impact on Organizations and Personnel**

**Documentation, Yearly Audits and Grades.** FISMA mandates that federal agencies are audited and graded annually. This had created a significant burden of paperwork and documentation. To make matters worse, many argue that in actual implementation FISMA measures the wrong things, such paperwork, but does not actually improve security.

### **Congressional Hearings and Lost of Reputation and Personal Responsibility**

**Congressional Hearings.** The leaders of the department must testify before Congress. In June 2006, ten senior Veteran Administration leaders were called to account before the House Committee on Veterans' Affairs.<sup>6</sup> While congressional hearings are can be unpleasant, follow-up actions are expensive. Senate Finance Committee Chairman Max Baucus (D-Mont.) called for the crackdown on accidental release of American social security numbers.<sup>7</sup> As shown in the private sector, security breaches can be costly, Forrester estimates range from \$90-305 per record loss in high-end industries such as banking.<sup>8</sup>

---

<sup>4</sup> Libby Quaid, AP Food and Farm Writer, "Hacker Breaks into Agriculture Department," *AP Online*, June 22, 2006.

<sup>5</sup> Report finds IRS Computer Flaws, *AP Online*, April 7, 2008

<sup>6</sup> U.S. Representative Steve Buyer (R-IN) Holds a Hearing on Department of Veteran Affairs Cyber-Security. At the hearing from the Veteran Affairs were Jim Nicholson (Secretary), Gordon Mansfield (Deputy Secretary), Dr. Jonathan Perlin (Undersecretary for Health), Ronald Aument (Deputy Secretary of Benefits), Major General Robert Howard (Acting Secretary for Information), Tim McClain (General Counsel), Tom Bowman (Chief of Staff), Dennis Duffy (Acting Assistant Secretary for Policy, Planning and Preparedness), Mark Whitney (Office of Policy, Planning and Preparedness), and from the National Cemetery Administration were William Tuerk (Undersecretary for Memorial Affairs).

<sup>7</sup> "Chairman Baucus Wants Crackdown on ID Security Breaches," US Fed News Services, April 24, 2007.

<sup>8</sup> Rebecca Susner, "Cyber Security: Data Breach Insurance Gains in Popularity: As data breaches become more frequent, insurance policies offer a range of protections. But should money spent on premiums be spent on shoring up security

**Other Investigations.** In the case of the VA's loss of a laptop with 26.5 million social security numbers, the Federal Bureau of Investigations and VA Inspector General have also launched full-scale investigations.<sup>9</sup>

**Personal and Organizational Responsibility.** There are also other burdens because agencies can be penalized for lower budgets, in addition to Congressional hearings. The Chief Information Security Officers and many other people inside organizations must bear personal responsibility for the security of the Agency's that they manage. This extends to contractors who are liable for security breaches.

### **Loss of Efficiency and Additional Pressures on Budget**

Cyber security and the need to protect information assets have led to a loss of efficiency that could be achieved as the perimeter needs to be protected, and breaches need to be remedied. The need to account for information assets has led to tremendous budgetary pressures.

**Loss of Efficiency.** As CISO's and their staff must be harden their systems and defend the perimeters of their systems, efficiency is impacted in a number of ways including (1) time and energy following up on security and (2) the limitation of productive activity such as telecommuting, and (3) lawsuits, even just their prevention.

After a security breach, the security and privacy of members throughout an agency must be checked. For example, in the case of the Department of Agriculture's breach of workers records, the privacy of all 110,000 of the Department's employees had to be reviewed.<sup>10</sup>

With traffic congestion in the Washington Metro Area, the federal government promoted telecommuting heavily in the 2000's, but because of security concerns, including the potential theft of laptops with sensitive data, and hackers intruding on remote user's wireless networks. The federal government posted a 7.3% drop in telecommuters from 2005 to 2006 because of a callback by the Department of Interior.<sup>11</sup>

In the case of the VA loss of 26.5 million records, a class-action lawsuit was filed by a collection of veterans groups demands that the VA disclose which personnel were affected by the theft,

---

instead?" *Bank Technology News and Source Media, Inc.*, June 1, 2007.

<sup>9</sup> Phillip Britt, "VA: Breach of Protocol (thief of the Veteran Affairs Department Laptop with Veterans' Data)," *Information Today*, September 1, 2006.

<sup>10</sup> Libby Quaid, AP Food and Farm Writer, "Hacker Breaks into Agriculture Department," *AP Online*, June 22, 2006.

<sup>11</sup> Sue Shellenbarger, "Some Companies Rethink Telecommunity Trend," *Maryland Gazette*, March 29, 2008.

and seeks \$1,000 who can show harm by the breach, amounting up to \$26.5 billion.<sup>12</sup>

**Budget.** In addition to the ambiguity of language in FISMA, the second difficulty facing Agency CISO's is low FISMA grades and the lack of funding to improve them.<sup>13</sup> The Congressional Budget Office estimates that the e-Government Reauthorization Act could cost that our government \$29 billion over a four-year period, mainly for securing the federal agencies' information systems.<sup>14</sup>

## **TOWARDS MEETING FISMA AND OTHER SECURITY CHALLENGES**

For government and public sector organizations, the challenges of maintaining a stable IT environment are significant. A growing number of users and applications make agencies susceptible to a host of IT challenges every day. At the same time, in addition to a variety of regulatory demands, such as the Federal Information Security Management Act (FISMA) of 2002, there is a real need to control costs. The need for a true solution, which would include continue monitoring and automatic is very clear.

### **Towards True Solution**

**Continuous Monitoring.** Real security involves not just regular audits but continuous monitoring throughout the year. Real security means staying abreast of the latest developments and addressing that they arise. Guidance for continuous monitoring can be found in publications such as NIST SP 800-37 and SP 800-53A. For now, continuous monitoring only means that controls are functioning as planned.<sup>15</sup>

**Automation.** In the current environment, the ability to monitor (collect, manage, and report) on the security of each agency is important, but the given the number of incidents in the current environment automatic resolution is almost a requirement.

### **Introduction to Triumfant**

Triumfant® is the leading provider of Automated Resolution Management™ software. Through Triumfant's IT Intelligence™ platform, IT executives and their staff can automatically

---

<sup>12</sup> Phillip Britt, "VA: Breach of Protocol (thief of the Veteran Affairs Department Laptop with Veterans' Data), *Information Today*, September 1, 2006.

<sup>13</sup> Grant Gross, "Survey: Gov't CISOs say FISMA Can Be Improved," *IDG New Services*, April 13, 2007.

<sup>14</sup> Matthew Weigelt, "Securing Info Systems Could Cost \$28 Billion, Budget Office Says," *Federal Computer Week*, December 4, 2007.

<sup>15</sup> See wikipedia, Federal Information Security Management Act of 2002.

discover, diagnose, and precisely repair any unwanted changes in your Microsoft Windows environment.

From Compliance to Security to Incident and Problem Management, Triumfant offers an easy-to-use solution that helps you reduce costs, mitigate risks and increase quality of service.

### **Challenges Met**

**Compliance.** Unlike other solutions that simply tell you when you're out of compliance, Triumfant® Compliance Manager™ puts you back in compliance and provides you with a verification report before you even know you were at risk. Staying ahead of audit and compliance needs include extensions to policy templates and reporting features specifically designed for compliance applications. Triumfant's Compliance Manager may be purchased with FISMA, FDCC, NIST SP800-68 and other privacy templates. It is possible to measure compliance to virtually any policy at any level of detail. New compliance reports allow compliance to be documented either by rule or by computer. In addition, Compliance Manager is SCAP compatible.

- Enforce any IT policy including: FISMA, FDCC, NIST 800-68 and custom IT policies.
- Maintain a perpetual state of compliance and audit-readiness.
- Be audit-ready at a moment's notice.

**Security Management.** Triumfant® Security Manager™ provides the last line of defense against malicious software against viruses, malware, rootkits, and whole host of zero-day attacks. Anti-virus software and firewalls are not enough to assure a secure IT environment. Security Manager's autonomic-based analytical abilities provide a response to previously unknown attacks. Security Manager is often the only way to maintain the integrity of your environment.

- Diagnose and remove zero-day attacks
- Stop the continuous stream of new viruses, spyware, adware and other malware to assure a secure IT environment.
- Security Manager succeeds where your anti-virus software fails, adding another security "layer of last resort" that can handle attacks where all other controls have failed.

**Resolution Management.** Triumfant® Resolution Manager™ reduces IT support costs, while keeping your IT environment without interruption and at peak performance. Resolution Manager minimizes the dependence on manual processes for identifying and resolving known and previously unknown IT issues, and usually achieves an average of one-third savings in IT support costs.

Resolution Manager reduces downtime and service desk calls by automatically identifying

issues before they turn into problems and incidents that result in service desk calls. As a result, user downtime and service desk calls can be reduced by an average of one-third.

Resolution Manager also supports Information Technology Infrastructure Library’s (ITIL) Best Practices. ITIL is a set of concepts and techniques for managing information technology infrastructure, development, and operations. Resolution Manager is the only solution offering fully automated incident and problem management capabilities that follow ITIL practices. Its analytic capabilities are indispensable for problem management, a portion of the ITIL model that many organizations are implementing today.

- Automatically detect and repair both known and unknown problems.
- Dramatically reduce service desk calls.
- Significantly reduce downtime.

	<b>Scanners</b>	<b>Configuration Tools</b>	<b>Triumphant</b>
<b>Continuous Scanning</b>	√	√	√
<b>Manual Configuration</b>		√	
<b>Auto Configuration</b>			√
<b>Auto-generated Audit of Configuration Changes</b>			√

## Conclusion

In recent years, security breaches and legislation have been critical in driving federal agencies to confront the nation’s cybersecurity issues. What is at stake is not only the personal and agency liabilities, but the confidence of the American people that the government can secure their most personal of information. Yet to secure not only the core, but periphery of even a small government agency, is a daunting task, and the IT budget increases often only cover a fraction of what needs to be done. Furthermore, with these budget increases are related paperwork, e.g., annual audits, and in net, resources for traditional support are not nearly enough.

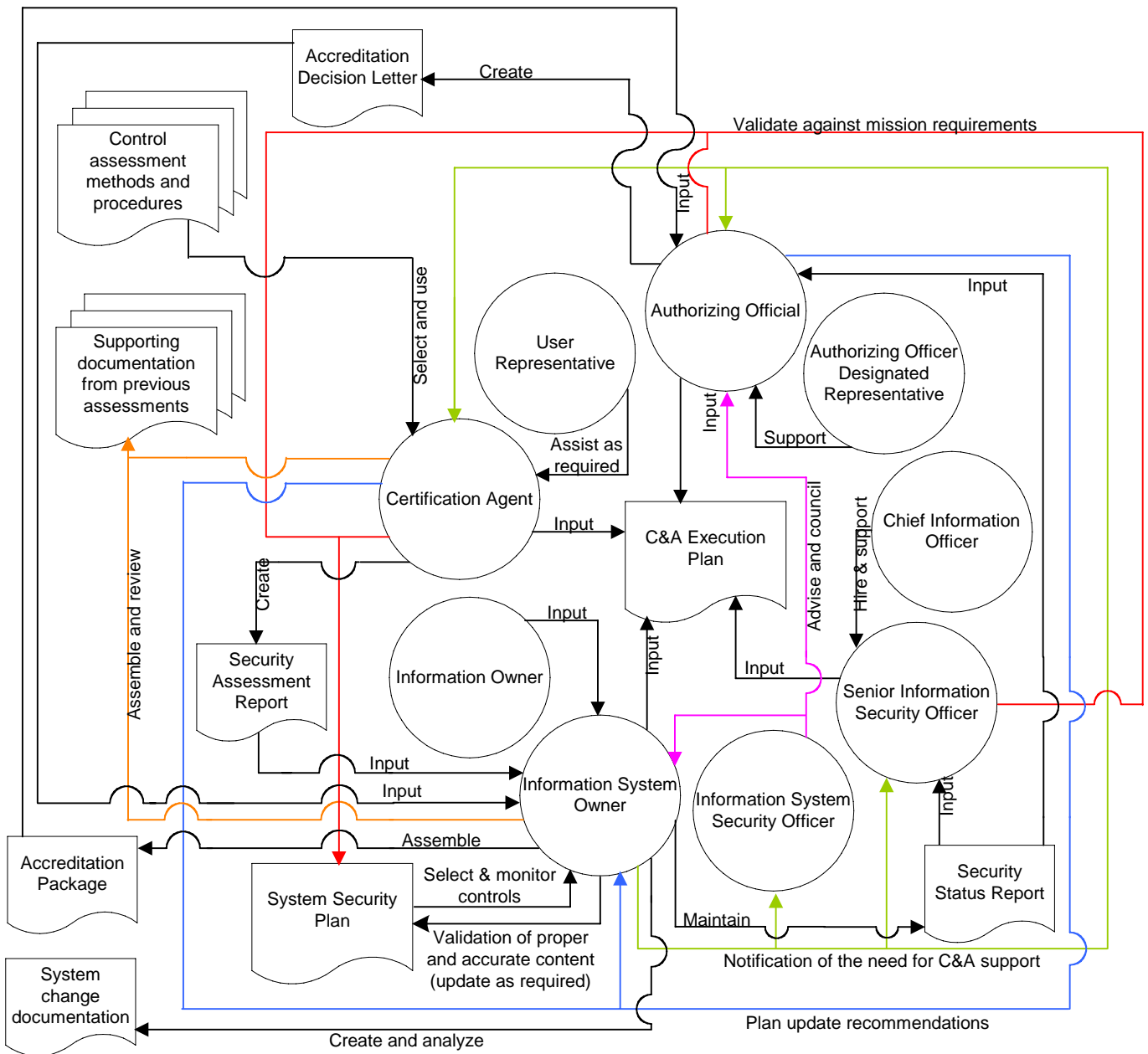
The need for automated controls has become apparent, as the number and variety of compliance requirements for every in-scope device make it practically impossible to otherwise maintain

compliance on an ongoing basis. Such controls must handle these requirements in both a technical and administrative sense, satisfying the control objectives while at the same time providing consistent, comprehensive reporting to address auditing requirements. The next generation of compliance and resolution management tools, such as those provided by Triumfant, can be a real solution in helping agencies officials to confront the nation's cybersecurity needs head on.

## Appendix A

### Capabilities of Triumfant – an agency official’s perspective

The capabilities of a solution like Triumfant can manifest in multiple and different ways when viewed through the eyes of different certification, accreditation and authorization officials. The entity relationship diagram below shows how the various roles defined by NIST 800-37 interact:



A general description of each relevant role is provided below.

- **Authorizing Official/Designated Representative (AO/DR)** (one per system, ultimate accountable official and typically the purse string holder)
  - Sometimes referred to as the Approving or Accrediting Authority
  - Senior management official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk
  - Assumes responsibility and is accountable for the risks associated with operating an information system
  - Typically has the authority to oversee the budget or business operations of the information system
  - May be called upon to approve system security requirements and system security plans
  - Can issue an interim approval to operate the system under specific terms and conditions
  - Can deny authorization to operate the system (or if the system is already operational, halt operations)
  
- **Chief Information Officer (CIO)** (Agency, Center, Directorate)
  - Management official responsible for:
    - designating a senior agency information security officer
    - developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements
    - training and overseeing personnel with significant responsibilities for information security
    - assisting management concerning their security responsibilities
    - reporting to senior management on the effectiveness of the information security program, including progress of remedial actions
  - Encourages the maximum reuse and sharing of security-related information including:
    - threat and vulnerability assessments
    - risk assessments
    - results from common security control assessments
    - any other general information that may be of assistance to information system owners
  - Determines the appropriate allocation of resources dedicated to the protection of information systems
  - May be designated as the authorizing official for agency-wide general support systems
  
- **Senior Agency Information Security Officer (SAISO)** (Headquarters)
  - Carries out the Chief Information Officer responsibilities under FISMA
  - Possesses professional qualifications, including training and experience, required to administer the information security program
  - Has information security duties as their primary duty
  - Heads an office with the mission and resources to assist in ensuring agency compliance with regulations and laws

- May also serve as the authorizing official's designated representative
- Serves as the Chief Information Officer's primary liaison to the authorizing officials, information system owners, and information system security officers
- **Information System Owner (ISO)** (a.k.a. System Owner, a civil servant)
  - Overall procurement, development, integration, modification, or operation and maintenance of an information system
  - Develops and maintains the system security plan
  - Ensures the system is deployed and operated according to the agreed upon security requirements
  - Decides who has access to the information system (and with what types of privileges or access rights)
  - Ensures that system users and support personnel receive security training (e.g., instruction in rules of behavior)
  - Informs management of the need to conduct a security Certification and Accreditation of the information system, ensures appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent
  - Receives the security assessment results from the certification agent
  - Assembles the accreditation package and submits the package to the authorizing official or the authorizing official's designated representative
- **Information Owner (IO)** (the business data owner)
  - Has legal or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal
  - Establishes the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations
  - Is not necessarily the same person as the information system owner (indeed, a single information system may utilize information from multiple information owners)
  - Should provide input to information system owners regarding the security requirements and security controls for the information systems where their information resides
- **Information System Security Officer (ISSO)** (one per system)
  - Responsible to the authorizing official, information system owner, or the senior information security officer for ensuring the appropriate operational security posture is maintained
  - Serves as the principal advisor to the authorizing official, information system owner, or senior information security officer on all matters involving the security of the information system
  - Has the detailed knowledge required to manage the security aspects of the information system and, in many cases, is assigned responsibility for the day-to-day security operations of the system

- May include physical security, personnel security, incident handling, and security training and awareness
- May be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis
- Plays an active role in developing and updating the system security plan and in managing and controlling changes to the system and assessing the security impact of those changes
- **Certification Agent (CA)** (third party assessor)
  - An individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
  - Provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system
  - Provides an independent assessment of the system security plan (prior to the assessment activities associated with the certification process) to ensure the plan provides a complete and consistent security specification for the information system that is adequate to meet all applicable security requirements
  - Should be independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system
  - Should be independent of those individuals responsible for correcting security deficiencies identified during the security certification

To the Authorizing Official/Designated Representative the deployment of the Triumphant solution provides a level of confidence and assurance that a significant number of critical controls are implemented on a consistent basis, operating effectively and producing the outcomes necessary to protect agency assets and missions. To the extent that systems contain data which must be protected at the FIPS-199 Moderate or High level, Triumphant addresses the control requirements that are invoked at those higher levels of data criticality relative to automation of control operations.

To the Chief Information Officer/Senior Agency Information Security Officer Triumphant represents a consistent, scalable solution to meet significant numbers of the required controls and control enhancements in a way that can be replicated across the agency/organization. It provides the basis for an assertion of control effectiveness continuous monitoring.

To the Information System Owner/Information Owner/Information System Security Officer Triumphant is a way to accomplish key security objectives in a cost effective and comprehensive way. The ROI associated with the Triumphant solution and the relative low cost associated with its deployment and staff training requirements make it an attractive alternative to enhance system security and provide adequate and accurate audit evidence in a timely fashion.

To the Certification Agent Triumphant presents a clear advantage in aligning audit requirements with tangible evidence of control operational effectiveness, in terms of both a snapshot at a moment in time as well as effectiveness over time.