BI and FISMA:
An Exploration of Information Security Functions

FISMA

EXECUTIVE SUMMARY:

FISMA — the Federal Information Security Management Act — is a U.S. law that directs how federal government agencies must protect information and information systems in support of three security objectives: integrity, confidentiality, and availability. By assigning security categories (low, moderate, high) and security objectives (integrity, confidentiality, availability) to information types and acquisition systems, agencies can satisfy minimum security requirements in seventeen security-related areas and comply with FISMA reporting requirements. Federal agencies use BI applications, including SAP BusinessObjects, to prepare, share, and/or publish information. Whether or not that information is shared within a BI solution, distributed outside it, or contains personally identifiable information (PII), the information is subject to FISMA. 360Suite, developed by Wiiisdom,is a set of software solutions that enhances SAP BusinessObjects by boosting efficiency, securing deployments, and delivering a deeper understanding of environments. The National Institute of Standards and Technology (NIST) cybersecurity framework, which establishes five functions as a means of organizing basic cybersecurity activities at their highest level, provides a logical structure for considering how BI solutions can be used in a manner that supports the goals and upholds the requirements of FISMA and how 360Suite can extend and enhance native capabilities.

WHAT IS FISMA?

FISMA stands for the Federal Information Security Management Act, a U.S. law passed in 2002 and amended in 2014 that requires federal agencies to protect "information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." FISMA was originally included as Title III of the E-Government Act of 2002, a broader law intended to "enhance the management and promotion of electronic Government services and processes" in order to "enhance citizen access to Government information and services." FISMA was enacted to ensure that information remained secure even as it became more accessible. It represents a conviction that information security is important to the economic and national security interests of the United States.

FISMA requires federal agencies to develop, document, implement, and maintain an information security program to protect its information and information systems, *including those provided or managed by other agencies, contractors, or sources.* (3544b)

Specifically, agencies must: (3544(a)(2)(A-D) and 35544(b)(1-8)

- Assess the risk and magnitude of harm that could result from unauthorized access to information or information systems;
- Determine the levels of information security appropriate to protect information and information systems;
- Develop and implement policies and procedures to cost-effectively reduce risk to an acceptable level;
- Train personnel, including contractors, in security awareness;
- Test and evaluate information security controls and techniques on a periodic basis;
- Develop a process to identify and address information security shortcomings;
- Develop procedures for detecting and responding to security incidents;
- Develop a plan to ensure the continuity of operations of information systems; and
- Ensure that information security is addressed throughout the life cycle of each agency information system.

HOW DO AGENCIES ASSIGN SECURITY CATEGORIES?

FISMA tasked the National Institute of Standards and Technology (NIST) with developing standards for categorizing information and information systems according to risk level in support of three security objectives:

1. **Integrity:** Guarding against improper information modification or destruction
2. **Confidentiality:** Preserving authorized restrictions on access and disclosure to protect personal privacy and proprietary information
3. **Availability:** Ensuring timely and reliable access to and use of information

For each of these three objectives, NIST assigned three levels of potential impact of security breaches on operations, assets or individuals, as outlined in Federal Information Processing Standards (FIPS) Publication 199.

1. Low (limited effect)
2. Moderate (serious effect)
3. High (severe/catastrophic effect)

To assign a security category to an information type (e.g., public, investigative, administrative), agencies must determine the potential impact (low, moderate, high, N/A) for each security objective (integrity, confidentiality, availability).

Information type: public
Security category of public information type = {(integrity, MODERATE), (confidentiality, N/A), (availability, LOW)}

To assign a security category to an information system, agencies must account for all information types that reside on the system. For each security objective, the system value is the highest value assigned to any individual information type. Consider, for example, an acquisition system that contains public, contract, and administrative information.

Information types: public, contract, administrative
Security category of acquisition system = {(integrity, HIGH), (confidentiality, HIGH), (availability, MODERATE)}

Note that the information system security category represents the highest value assigned to each security objective across all information types contained therein.

Information Type	Integrity	Confidentiality	Avaibility
Public	MODERATE	LOW*	LOW
Contact	HIGH	MODERATE	MODERATE
Administrative	MODERATE	HIGH	LOW

** N/A is not an option when assigning values to information types for the purpose of determining the information system security category.*

WHAT ARE THE MINIMUM SECURITY REQUIREMENTS?

FISMA also tasked NIST with defining minimum information security requirements. As outlined in FIPS PUB 200 and detailed in NIST Special Publication 800-53, NIST established minimum security requirements for information and information systems in seventeen security-related areas:

1. Access control: Limit information system access to authorized users.
2. Awareness and training: Train users and managers in risks and requirements.
3. Audit and accountability: Create information system audit records. Be able to trace individual users to specific actions.
4. Certification, accreditation, and security assessments: Assess and monitor security controls, and develop a plan to correct deficiencies.
5. Configuration management: Establish baseline configurations and inventories of information systems.
6. Contingency planning: Establish and maintain DR and backup plans to ensure continuity of operations in case of emergencies.
7. Identification and authentication: Verify the identity of information system users before granting them access.
8. Incident response: Track, document, and report incidents as required.
9. Maintenance: Maintain information systems.
10. Media protection: Protect information system media.
11. Physical and environmental protection: Limit physical access to information systems (equipment and infrastructure) to authorized people and protect them from environmental hazards.
12. Planning: Develop, document, and implement security plans for information systems.
13. Personnel security: Ensure that people in positions of responsibility (including third-parties) are trustworthy.
14. Risk assessment: Periodically assess the risk to operations, assets, and individuals resulting from information systems.
15. System and services acquisition: Establish guidelines for software installation and usage, and ensure that third-parties protect information.
16. System and communications protection: Monitor, control and protect organizational communications.
17. System and information integrity: Identify, report, and correct information and information system flaws.

WHAT ARE THE REPORTING REQUIREMENTS?

Every federal agency is responsible for complying with FISMA requirements and reporting annually on the adequacy and effectiveness of its information security policies, procedures, and practices. FISMA 2014 expanded reporting requirements by specifically requiring agencies to produce an annual report that includes:

- A description of each major IS incident, including: summaries of the threats, threat actors, vulnerabilities and impacts; the risk assessments before the incident date; the status of compliance with requirements at the time of the incident; and an explanation of detection, response, and remediation efforts;

- The total number of IS incidents, impact levels, types, and locations of affected systems; and

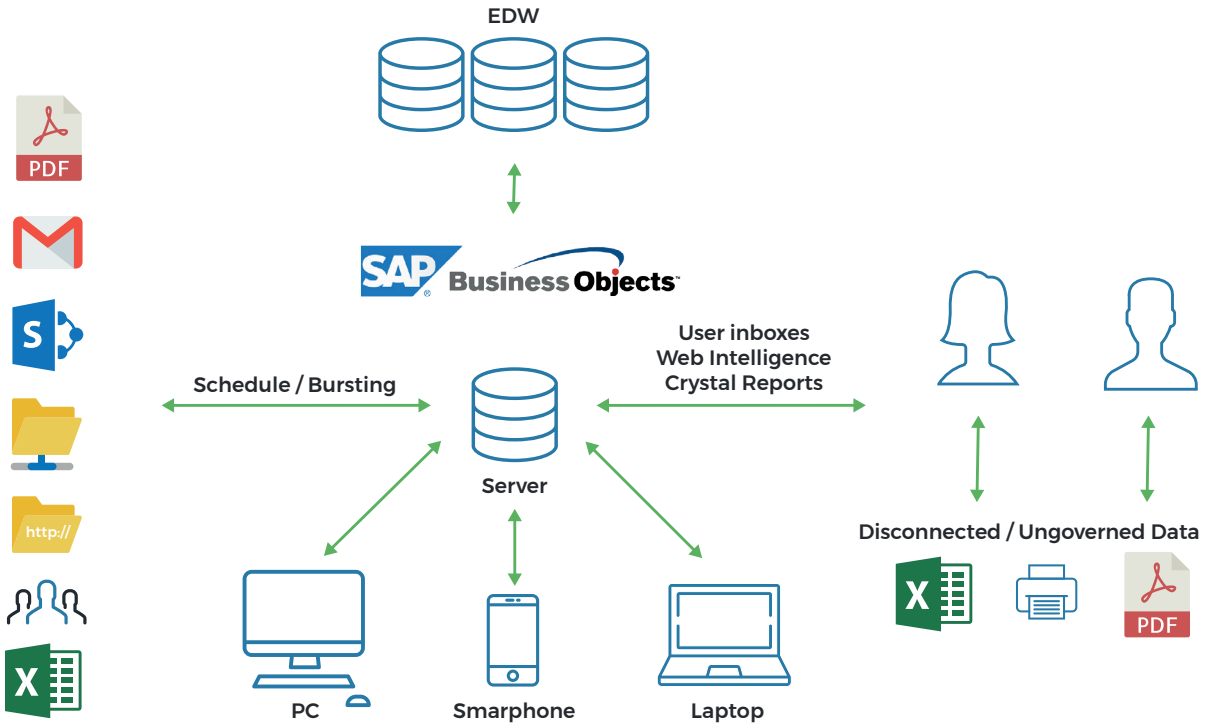
- A description of each major IS incident involving personally identifiable information (PII), including the number of people affected and a description of the information that was breached/exposed.

In addition, in the event of a major incident, FISMA 2014 requires agencies to notify numerous committees of Congress no more than seven days after the incident and whenever new information is uncovered. It's worth noting that separate reporting requirements apply to national security systems.

WHAT'S THE RELATIONSHIP BETWEEN FISMA AND BUSINESS INTELLIGENCE?

Forrester defines Business intelligence (BI) as "a set of methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information used to enable more effective strategic, tactical, and operational insights and decision-making" (Evelson, 2008). Business intelligence applications (e.g, SAP BusinessObjects, Tableau, Power BI, etc.) support this process by retrieving, analyzing, transforming, and reporting on data (potential information) and generating metadata (statements about that information). Federal agencies use BI applications to obtain data from multiple database warehouses via the ETL process and prepare, share, and/or publish information, which makes BI critical for FISMA.

Whether or not that information is shared within a BI solution, distributed outside it, or contains personally identifiable information (PII), the information is subject to FISMA. BI solutions also generate new information, for example, about BI users and report recipients, that is also subject to FISMA. Finally, BI solutions are acquisitions that fall under the NIST "system and services acquisition" category for the purpose of applying minimum security requirements. **As such, BI solutions must be used in a manner that supports the goals and upholds the requirements of FISMA.**



Example of Business Intelligence Data Flow in SAP BusinessObjects. BI involves multiple data sources, data is compiled and shared both within BI application users, or outside of BI applications becoming ungoverned content. Being able to trace data flow and security is key to complying with FISMA requirements.

NIST CYBERSECURITY FRAMEWORK

In 2013, the government and private sector collaborated to develop a cybersecurity framework in response to Executive Order 13636. It uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The framework establishes five functions as a means of organizing basic cybersecurity activities at their highest level.

1. **Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. **Respond**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Although outside the scope of FISMA, the five functions framework, modified slightly for BI relevance, provides a logical structure for considering how BI solutions can be used in a manner that supports the goals and upholds the requirements of FISMA.

WHAT IS 360SUITE?

360Suite by GB&SMITH is a set of software solutions that enhance SAP BusinessObjects by boosting efficiency, securing deployments, and delivering a deeper understanding of environments. Serving more than 3 million end-users worldwide, 360Suite helps companies and government organizations ensure that SAP BusinessObjects supports policies related to governance, risk management, and regulatory compliance.

FUNCTION #1: IDENTIFY / FIND

Managing the information security risks of BI applications requires a complete understanding of BI platforms. Agencies must be able to answer questions like:

- Who has access to BI solutions? (Ideally, agencies should be able to correlate users and IP addresses for extra security.)
- What are the data sources of BI information?
- What are the security categories of BI information types?
- With whom and how are BI reports shared?
- Are BI servers configured for third-party authentication (aliases) (e.g., LDAP, AD, SAP)?
- What is the BI ETL transformation architecture (e.g., multistage, in-warehouse)?
- What metadata passes from source to BI solution?
- Is BI content governed (i.e., does it retain native security settings when shared outside a BI solution)?

360Suite exposes metadata that make it possible to:

- Identify BI users and their IP addresses
- Map BI data sources
- Data Catalog BI content
- Tag BI content according to risk level (low, moderate, high)
- Tag BI content by security objective (integrity, confidentiality, availability)
- Tag personally identifiable information (PII) objects
- Map BI report scheduling, destinations, and formats
- Document BI objects
- Understand the configuration of BI applications, including OS systems and server locations
- Understand the different BI environments (e.g., dev, prod, test) and their locations
- Understand the schema of BI databases (audit, CMS, reporting)

360Suite also documents metadata in the form of dozens of prebuilt and customizable WebI reports.

Learn how to implement and use tags in SAP BusinessObjects

FUNCTION #2: PROTECT / SECURE

After understanding BI platforms, agencies must develop and implement appropriate safeguards to protect them. An essential component of protection is access control. In the context of FISMA, access control means limiting information system access to authorized users. In order to limit access to BI, agencies must fully understand BI security settings.

360Suite includes a unique and patented security matrix that provides a complete picture of security, including:

- User accounts and access levels
- Users with large amount of rights
- Users by type (e.g., power users, administrators, report developers)
- User by group
- Inheritances, including multiple and broken inheritances
- Access rights to critical documents and objects

By visualizing security, 360Suite also helps agencies consider how the status of critical documents and user access requirements may change over time so they can plan out the lifecycle of users and information.

Another essential component of protection is data security. BI reports are often shared externally in insecure formats, such as PDF or XLS. 360Suite makes it possible to enhance information security through:

- Data and user pseudonymization
- Password protections
- Watermarks
- Metadata tagging
- Embedded footnotes containing owner information and security classification

FUNCTION #3: DETECT / MONITOR

In addition to protecting BI platforms, agencies must develop and implement the appropriate activities to recognize when BI information security has been compromised. This requires continuous monitoring of all BI content, which supports the detection process.

The best way to monitor BI applications is by leveraging BI on BI — analyzing BI metadata in search of changes over time as indicated by activity and non-activity related to users, security settings, and content.

BI on BI should be:

- Applied to all BI applications, of which most agencies use several
- Centralized in a single metadata services application
- Made available to artificial intelligence (AI) for the purpose of prescriptive analytics (suggested decision options based on the results of descriptive and predictive analytics)

By exposing BI metadata, 360Suite makes it possible to:

- Compare metadata changes over time to track activity and — just as important — non-activity on objects and documents;
- Map actions and objects to users for non-repudiation (i.e., a connection that cannot be denied)
- Manage the workflow of sensitive content to audit actions and approvals, compare objects before and after promotions, and roll back content when necessary
- Perform regression testing on data and metadata to ensure BI system and information integrity
- Generate automated reports to be used as the basis for account recertification: cross-checking names with control forms, verifying lists with supervisors, modifying or terminating user accounts as appropriate, and documenting the process
- Perform impact analysis to understand the full lineage (database to BI solution via the ETL process) and the effect on documents of modifying objects.
- Automate reporting on BI content, users, usage, non-usage, sources and sharing

Note that Federal Agency cloud deployments and service models at the low, moderate, and high risk impact levels are subject to the Federal Risk and Authorization Management Program (FedRAMP) in addition to FISMA.

FUNCTIONS #4 & 5: RESPOND & RECOVER

Finally, agencies must develop and implement the appropriate activities to take action and restore services when BI information security is compromised. Specific activities include contingency planning and maintaining backups. The goal of contingency planning is to ensure continuity of operations. Backups help manage disruptions and prevent destruction.

NIST Special Publication 800-34 Rev. 1 explains the difference between information security contingency plans (ISCP) and disaster recovery plans (DRP). Whereas DRPs are site-specific and focused on moving damaged operations to temporary, alternate locations, ISCPs provides key information for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system, no matter where the operations are located. Restoring a BI system after information security is compromised involves restoring BI applications as well as databases. Agencies must test ISCPs to ensure they are effective and don't exceed the maximum tolerable downtown (MTD) for continuity of operations (COOP).

360Suite facilitates contingency planning by taking snapshots of BI platforms on a regular basis. This provides metadata related to objects, users, security, scheduling, and more. When a BI information security incident initiates disaster recovery (DR) procedures, 360Suite snapshots make it possible to ensure that pre-DR and post-DR environments are identical. 360Suite snapshots also make it possible to restore data when maintenance activities, such as patches, updates, migrations, and ETL changes, unintentionally impact services.

Organizations typically back up entire BI servers and CMS databases. With this approach, it's possible to restore a system as a whole but not to roll back selectively or restore individual objects. With full backups, data that was modified or deleted after the time of the last backup will revert to a prior state when the BI server is restored. Full backups also fail to consider that, if an environment becomes corrupted, mirrored backups will also be corrupted, whether on the server, a VM, or in the cloud. Finally, full backups impact platform availability, potentially for long periods of time.

360Suite solves this problem with incremental backups that make it possible to restore previous versions of any object in any folder at any time if BI information security is compromised. By empowering agencies to restore specific content in seconds and full environments in minutes or hours, 360Suite supports continuity of operations and the FISMA security objectives of integrity and availability.

BI solutions tend to create multiple instances of the same document, which multiplies the risk to information security. In a typical BI environment, 40-60% of content can be archived without impacting users. 360Suite makes it easy to classify instances and documents by age and usage/non-usage, and to automatically archive content at the end of its lifespan. 360Suite also makes it possible to restore archived instances in the right format and in their proper location if it becomes necessary to satisfy information security requirements.

CONCLUSION

Most, if not all, federal agencies rely on BI to turn raw data into useful and shareable information. The data that BI touches and the information it generates is subject to FISMA. In addition, BI applications are part of larger federal information systems that are themselves subject to FISMA. BI can and should be used to uphold the requirements of FISMA, but native BI capabilities are typically insufficient to achieve these goals.

FISMA is often criticized as being just a checklist. Effective implementation requires agencies to find, protect, and monitor information, and to respond quickly when information security comes under threat. BI applications are good at retrieving, analyzing, transforming, and reporting on data, but they are not as good at keeping data secure.

360Suite enhances SAP BusinessObjects by exposing BI metadata that makes it easier for agencies to secure information. Metadata enables agencies to understand, map, and document BI users, data sources, content, servers, environments, and more. It also allows agencies to protect and monitor BI applications by enhancing security and revealing actions/non-actions and changes over time. Finally, it enables automated regression testing and supports incremental back ups, which make it possible for agencies to find and fix inconsistencies. When it comes to FISMA, 360Suite makes BI safer.

360Suite is a suite of **agile governance solutions** for SAP BusinessObjects developed by Wiiisdom.

At Wiiisdom, we transform your **Analytics landscape** into a **reliable** place to make **better, trusted decisions** every day and maximize your data assets.

360Suite is a set of solutions to ensure **quality, reliability, performance, and efficiency** of SAP BusinessObjects through testing, auditing, monitoring, cataloging, and scheduling methodologies. 360Suite is designed for large organizations looking to **mitigate data risks**, automate operations, and is the solution of choice for any migration project.

REFERENCES

FISMA 2002
FISMA 2014
NIST FIPS PUB 199
NIST FIPS PUB 200
NIST Special Publication 800-53

REQUEST A DEMO

Author:
Bruno Masek

Content Writer:
Kristen Gray

Be **FISMA** ready with **360Suite**

FISMA

360 Suite

Visit https://wiiisdom.com/360suite/