BOMGAR™

Vulnerability Scans
Privileged Access 18.2

TC:6/8/2018

BOMGAR
ENTERPRISE REMOTE SUPPORT

18.2.1 Privileged Access Management FISMA Compatibility

This report includes important security information about Bomgar 18.2.1 Privileged Access Management

[US] Federal Information Security Mgmt. Act (FISMA) Compliance Report

This report was created by IBM Security AppScan Standard 9.0.3.7 iFix004, Rules: 12676
Scan started: 6/8/2018 1:55:02 PM

Regulations

Federal Information Security Management Act (FISMA)

Summary

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the Electronic Government Act of 2002. It provides a framework to ensure comprehensive measures are taken to secure federal information and assets. It requires each federal agency to develop, document, and implement an agency-wide 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.

The Office of Management and Budget (OMB) requires federal agencies to prepare Plans of Action and Milestones Process (POA and Ms) reports for all programs and systems where they have found an IT security weakness. CIOs and agency program officials must develop, implement, and manage POA and Ms for all programs and systems they operate and control. Program officials must regularly update the agency CIO on their progress so the CIO can monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

Agencies must submit a report to the OMB that summarizes the results of annual IT security reviews of systems and programs, and any progress the agency has made towards fulfilling their FISMA goals and milestones.

OMB uses the reports to help evaluate government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform development of the E-Government Scorecard under the President's Management Agenda. The report must summarize the results of annual IT security reviews of systems and programs, and any progress the agency has made towards fulfilling their FISMA goals and milestones.

FISMA requires that federal agency officials understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

FISMA Implementation

Phase I: Standards and Guidelines Development

The first phase of the FISMA Implementation Project focuses on the development and updating of the security

standards and guidance required to effectively implement the provisions of the legislation. The implementation of the NIST standards and guidance will help agencies create and maintain robust information security programs and effectively manage risk to agency operations, agency assets, and individuals.

Phase II: Implementation and Assessment Aids

The second phase of the FISMA Implementation Project is focused on providing information system implementation and assessment reference materials for building common understanding in applying the NIST suite of publications supporting the Risk Management Framework (RMF).

NIST Implementation Documents

NIST develops and issues standards, guidelines and other publications to assist federal agencies in implementing FISMA, including minimum requirements, for providing adequate information security for all agency operations and assets but such standards and guidelines shall not apply to national security systems.

Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies. FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use. FIPS 200 mandates the use of Special Publication 800-53, as amended.

AppScan and FISMA

AppScan's FISMA compliance report will automatically detect possible issues in your Web environment that may be relevant to your overall compliance with the minimum security controls recommendations as set in the security catalog of NIST Special Publication 800 53. This report was constructed according to the HIGH-IMPACT Information Systems baseline. Organizations that use low or moderate control baseline may have to adjust the results accordingly.

Covered Entities

All Federal agencies and organizations which possess or use Federal information -- or which operate, use, or have access to Federal information systems -- on behalf of a Federal agency, including contractors, grantees, State and local governments, and industry partners.

Effective Date

December 2002

Compliance Required by

Federal agencies must submit their annual IT review reports to the OMB by October of each year.

Regulators/Auditors

The Office of Management and Budget (OMB).

For more information on securing web applications, please visit: http://www-03.ibm.com/software/products/en/category/application-security

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Issues detected across 0/23 sections of the regulation:

Sections	Number of Issues
Sec.3544.(A), Sec.3547(1) - The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;	0
Sec.3544.(B) - The head of each agency shall be responsible for complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—(i) information security standards promulgated under section 11331 of title 40; and (ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President;	0
NIST SP 800_53,AC-3 - The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	0
NIST SP 800_53,AC-6 - The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	0
NIST SP 800_53,AC-10 - The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	0
NIST SP 800_53,AC-11 - The Organization prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures.	0
NIST SP 800_53,AC-17 - The organization: Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and Authorizes remote access to the information system prior to allowing such connections.	0
NIST SP 800_53,CM-6 - The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and	0

approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
NIST SP 800_53,CM-7 - The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	0
NIST SP 800_53,IA-2 - The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	0
NIST SP 800_53,IA-4.D - The organization manages information system identifiers for users and devices by preventing reuse of user or device identifiers for [Assignment: organization-defined time period].	0
NIST SP 800_53,IA-4.E - The organization manages information system identifiers for users and devices by disabling the user identifier after [Assignment: organization-defined time period of inactivity].	0
NIST SP 800_53,IA-5.C - The organization manages information system authenticators for users and devices by ensuring that authenticators have sufficient strength of mechanism for their intended use.	0
NIST SP 800_53,IA-5.E - The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation.	0
NIST SP 800_53,RA-5.A - The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported.	0
NIST SP 800_53,SC-5 - The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].	0
NIST SP 800_53,SC-8 - The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	0
NIST SP 800_53,SC-13 - The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	0
NIST SP 800_53,SC-23 - The information system protects the authenticity of communications sessions.	0
NIST SP 800_53,SI-3.A - Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;	0
NIST SP 800_53,SI-3.B - The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;	0
NIST SP 800_53,SI-10 - The information system checks the validity of information inputs.	0
NIST SP 800_53,SI-11.A - Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries;	0

Section Violation By Issue

0 Unique issues detected across 0/23 sections of the regulation:

URL	Entity	Issue Type	Sections

Detailed Security Issues by Sections

Sec.3544.(A), Sec.3547(1) - The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; 0

Sec.3544.(B) - The head of each agency shall be responsible for complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—(i) information security standards promulgated under section 11331 of title 40; and (ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; 0

NIST SP 800_53,AC-3 - The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. 0

NIST SP 800_53,AC-6 - The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. 0

NIST SP 800_53,AC-10 - The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. 0

NIST SP 800_53,AC-11 - The Organization prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures. 0

NIST SP 800_53,AC-17 - The organization: Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and Authorizes remote access to the information system prior to allowing such connections. 0

NIST SP 800_53,CM-6 - The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. 0

NIST SP 800_53,CM-7 - The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. 0

NIST SP 800_53,IA-2 - The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). 0

NIST SP 800_53,IA-4.D - The organization manages information system identifiers for users and devices by preventing reuse of user or device identifiers for [Assignment: organization-defined time period]. 0

NIST SP 800_53,IA-4.E - The organization manages information system identifiers for users and devices by disabling the user identifier after [Assignment: organization-defined time period of inactivity]. 0

NIST SP 800_53,IA-5.C - The organization manages information system authenticators for users and devices by ensuring that authenticators have sufficient strength of mechanism for their intended use. 0

NIST SP 800_53,IA-5.E - The organization manages information system authenticators for users and devices by changing default content of authenticators upon information system installation. 0

NIST SP 800_53,RA-5.A - The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported. 0

NIST SP 800_53,SC-5 - The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards]. 0

NIST SP 800_53,SC-8 - The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. 0

NIST SP 800_53,SC-13 - The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. 0

NIST SP 800_53,SC-23 - The information system protects the authenticity of communications sessions. 0

NIST SP 800_53,SI-3.A - Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; 0

NIST SP 800_53,SI-3.B - The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; 0

NIST SP 800_53,SI-10 - The information system checks the validity of information inputs. 0

NIST SP 800_53,SI-11.A - Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; 0

BOMGAR
ENTERPRISE REMOTE SUPPORT

18.2.1 Privileged Access Management Web Application Report

This report includes important security information about Bomgar 18.2.1 Privileged Access Management

OWASP Top 10 2017 Report

This report was created by IBM Security AppScan Standard 9.0.3.7 iFix004, Rules: 12676
Scan started: 6/8/2018 1:55:02 PM

Regulations

OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks

Summary Description

The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. Development projects should address these potential risks in their requirements documents and design, build and test their applications to ensure that they have taken the necessary measures to reduce these risks to the minimum. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review as part over the overall effort to address the risks.

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security risks. The Top 10 provides basic guidance on how to address against these risks and where to go to learn more on how to address them.

Although setout as an education piece, rather than a standard or a regulation, it is important to note that several prominent industry and government regulators are referencing the OWASP top ten. These bodies include among others VISA USA, MasterCard International and the American Federal Trade Commission (FTC).

However, according to the OWASP team the OWASP top ten first and foremost an education piece, not a standard. The OWASP team suggests that any organization about to adopt the Top Ten paper as a policy or standard to consult with the OWASP team first.

What Changed From 2013 to 2017?

The threat landscape for applications and APIs constantly changes. Key factors in this evolution are the rapid adoption of new technologies (including cloud, containers, and APIs), the acceleration and automation of software development processes like Agile and DevOps, the explosion of third-party libraries and frameworks, and advances made by attackers. These factors frequently make applications and APIs more difficult to analyze, and can significantly change the threat landscape. To keep pace, the OWASP organization periodically update the OWASP Top 10. In this 2017 release, following changes were made:

Merged 2013-A4: "Insecure Direct Object References" and 2013-A7: "Missing Function Level Access Control" into 2017-A5: "Broken Access Control".

Dropped 2013-A8: "Cross-Site Request Forgery (CSRF)" as many frameworks include CSRF defenses, it was found in only 5% of applications.

Dropped 2013-A10: "Unvalidated Redirects and Forwards", while found in approximately in 8% of applications, it was edged out overall by XXE.

Added 2017-A4: "XML External Entities (XXE)".

Added 2017-A8: "Insecure Deserialization".

Added 2017-A10: "Insufficient Logging and Monitoring".

Covered Entities

All companies and other entities that develop any kind of web application code are encouraged to address the top ten list as part of their over all security risk management. Adopting the OWASP Top Ten is an effective first step towards changing the software development culture within the organization into one that produces secure code.

For more information on OWASP Top Ten, please review the - OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks, at http://www.owasp.org

For more information on securing web applications, please visit http://www-03.ibm.com/software/products/en/category/application-security

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Issues detected across 0/10 sections of the regulation:

Sections	Number of Issues
A1 - Injection	0
A2 - Broken authentication	0
A3 - Sensitive Data Exposure	0
A4 - XML External Entities (XXE)	0
A5 - Broken Access Control	0
A6 - Security Misconfiguration	0
A7 - Cross site scripting (XSS)	0
A8 - Insecure Deserialization	0
A9 - Using Components with Known Vulnerabilities	0
A10 - Insufficient Logging and Monitoring	0

Section Violation By Issue

0 Unique issues detected across 0/10 sections of the regulation:

URL	Entity	Issue Type	Sections

Detailed Security Issues by Sections

A1 - Injection 0

A2 - Broken authentication 0

A3 - Sensitive Data Exposure 0

A4 - XML External Entities (XXE) 0

A5 - Broken Access Control 0

A6 - Security Misconfiguration 0

A7 - Cross site scripting (XSS) 0

A8 - Insecure Deserialization 0

A9 - Using Components with Known Vulnerabilities 0

A10 - Insufficient Logging and Monitoring 0

BOMGAR
ENTERPRISE REMOTE SUPPORT

18.2.1 Privileged Access Management PCI Compatibility

This report includes important security information about Bomgar 18.2.1 Privileged Access Management

The Payment Card Industry Data Security Standard (PCI DSS) Compliance Report

This report was created by IBM Security AppScan Standard 9.0.3.7 iFix004, Rules: 12676
Scan started: 6/8/2018 1:55:02 PM

Regulations

The Payment Card Industry Data Security Standard (PCI) Version 3.2

Summary

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.

“System components” include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following: Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.

Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).

Applications including all purchased and custom applications, including internal and external (for example, Internet) applications. Any other component or device located within or connected to the CDE.

Covered Entities

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE1. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

Compliance Penalties

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, the card companies may fine the acquiring member, or impose restrictions on the merchant or its agent.

Compliance Required By

PCI DSS version 3.2 has replaced PCI DSS v.2 and is effective as of January 1st 2014. The PCI DSS v.2 may not be used for PCI DSS compliance after December 31, 2014.

Regulators

The PCI Security Standards Council, and its founding members including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

For more information on the PCI Data Security Standard, please visit:

https://www.pcisecuritystandards.org./index.htm

For more information on securing web applications, please visit http://www-01.ibm.com/software/rational/offerings/websecurity/

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Issues detected across 0/32 sections of the regulation:

Sections	Number of Issues
Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters.	0
Requirement 2.1 - Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.)	0
Requirement 2.2.2 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	0
Requirement 2.2.4 - Configure system security parameters to prevent misuse.	0
Requirement 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems.	0
Requirement 2.3 - Encrypt all non-console administrative access using strong cryptography. Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	0
Requirement 2.6 - This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data.	0
Requirement 4 - Encrypt transmission of cardholder data across open, public networks.	0
Requirement 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use. Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	0
Requirement 6 - Develop and maintain secure systems and applications.	0
Requirement 6.1 - Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	0
Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1	0
Requirement 6.3 - Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	0
Requirement 6.3.1 - Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	0
Requirement 6.4.4 - Removal of test data and accounts from system components before the system becomes active / goes into production.	0
Requirement 6.5 - Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	0
Requirement 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection,	0

LDAP and XPath injection flaws as well as other injection flaws.	
Requirement 6.5.2 - Buffer overflow	0
Requirement 6.5.3 - Insecure cryptographic storage	0
Requirement 6.5.4 - Insecure communications	0
Requirement 6.5.5 - Improper error handling	0
Requirement 6.5.7 - Cross site scripting (XSS)	0
Requirement 6.5.8 - Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	0
Requirement 6.5.9 - Cross site request forgery (CSRF)	0
Requirement 6.5.10 - Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement	0
Requirement 6.6 - For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	0
Requirement 7 - Restrict access to data by business need-to-know	0
Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access.	0
Requirement 7.1.2 - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	0
Requirement 8.2 - In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	0
Requirement 8.2.1 - Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	0
Requirement 8.7 - All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	0

Section Violation By Issue

0 Unique issues detected across 0/32 sections of the regulation:

URL	Entity	Issue Type	Sections

Detailed Security Issues by Sections

Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters. 0

Requirement 2.1 - Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.) 0

Requirement 2.2.2 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system. 0

Requirement 2.2.4 - Configure system security parameters to prevent misuse. 0

Requirement 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. 0

Requirement 2.3 - Encrypt all non-console administrative access using strong cryptography. Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. 0

Requirement 2.6 - This section applies to web applications that are used by hosting providers for hosting purposes – Hosting providers must protect each entity's hosted environment and data. 0

Requirement 4 - Encrypt transmission of cardholder data across open, public networks. 0

Requirement 4.1 - Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use. Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. 0

Requirement 6 - Develop and maintain secure systems and applications. 0

Requirement 6.1 - Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. 0

Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1 0

Requirement 6.3 - Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party. 0

Requirement 6.3.1 - Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. 0

Requirement 6.4.4 - Removal of test data and accounts from system components before the system becomes active / goes into production. 0

Requirement 6.5 - Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. 0

Requirement 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. 0

Requirement 6.5.2 - Buffer overflow 0

Requirement 6.5.3 - Insecure cryptographic storage 0

Requirement 6.5.4 - Insecure communications 0

Requirement 6.5.5 - Improper error handling 0

Requirement 6.5.7 - Cross site scripting (XSS) 0

Requirement 6.5.8 - Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). 0

Requirement 6.5.9 - Cross site request forgery (CSRF) 0

Requirement 6.5.10 - Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement 0

Requirement 6.6 - For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. 0

Requirement 7 - Restrict access to data by business need-to-know 0

Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access. 0

Requirement 7.1.2 - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. 0

Requirement 8.2 - In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric. 0

Requirement 8.2.1 - Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. 0

Requirement 8.7 - All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). 0

BOMGAR
ENTERPRISE REMOTE SUPPORT

18.2.1 Privileged Access Management GDPR Compatibility

This report includes important security information about Bomgar 18.2.1 Privileged Access Management

[EU] Regulation 2016/679 Of The European Parliament And Of The Council (GDPR) Compliance Report

This report was created by IBM Security AppScan Standard 9.0.3.7 iFix004, Rules: 12676
Scan started: 6/8/2018 1:55:02 PM

Regulations

Regulation 2016/679 Of The European Parliament And Of The Council - General Data Protection Regulation (GDPR)

General - EU Directive Applicability

A European Union Directive is the collective decision made by the member states, acting through their national Government Ministers in the Council of the European Union and the Parliament.

A directive fixes the objectives to be pursued by the EU member states, but leaves freedom of choice for the ways of obtaining them (maintaining an obligation to achieve the result). How each country puts the directive into effect depends on their legal structure, and may vary.

In practice, the Union 'addresses' directives to all member states, and specifies a date by which the states must have put the directive into effect. (These dates are determined by the Council of Ministers at the time of the main agreement). Individual states often miss these deadlines, and when the deadlines slip badly, the European Commission can and does commence proceedings in the European Court of Justice against the countries involved.

Through its case law, the European Court of Justice has provided guidelines for member state judges on how to deal with cases where directives have not been transposed into national law, or have been transposed incorrectly.

When national law has multiple possible interpretations, the judge must choose the interpretation that conforms with EU law. This rule also applies to directives not yet transposed into national law.

In cases against the state or any state body, directives have "direct effect". A state that hasn't transposed a directive on time may not invoke this to its own benefit. "Direct effect" only applies to rules that are sufficiently clear.

Citizens can sue the state for damages caused because of tardy transposition.

Infractions - Where a Member State fails to comply with its obligations under the Treaty - for example, by not correctly transposing a directive (or not doing so on time), or by failing to implement it properly. Infraction cases are taken to the European Court of Justice by the Commission for trial if their Reasoned Opinion is not adequately answered.

Unlike a directive this regulation does not require any enabling legislation to be passed by governments.

Summary

This regulation's main objective is to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

'Personal Data' means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing of Personal Data' (or 'Processing') means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Applicability

The regulation applies if the data controller or processor (organization) or the data subject (person) is based in the EU. Furthermore the Regulation also applies to organizations based outside the European Union if they process personal data of EU residents. The regulation does not apply to the processing of personal data for national security activities or law enforcement.

Compliance Penalties

Determined by each member state, but may include:

A warning in writing in cases of first and non-intentional non-compliance

Regular periodic data protection audits

A fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

A fine up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Effective Date

The regulation was adopted on 27 April 2016. It enters into application 25 May 2018 after a two-year transition period.

For more information on securing web applications, please visit http://www-03.ibm.com/software/products/en/appscan .

Violated Section

Issues detected across 0/4 sections of the regulation:

Sections	Number of Issues
Article 25(1) - Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	0
Article 32(1)(a) - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data.	0
Article 32(1)(b) - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	0
Article 32(2) - In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed	0

Section Violation By Issue

0 Unique issues detected across 0/4 sections of the regulation:

URL	Entity	Issue Type	Sections

Detailed Security Issues by Sections

Article 25(1) - Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 0

Article 32(1)(a) - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data. 0

Article 32(1)(b) - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. 0

Article 32(2) - In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed 0