RSA Security® Best Practices Framework

Building a strategic approach to compliance

As the number of regulations mandating the protection of information continues to grow, companies and government agencies must figure out how to streamline their compliance efforts. Contrary to a tactical approach, which tries to meet the requirements of each regulation separately, a strategic approach looks at compliance holistically, and combines efforts across all of the various regulations - SOX, PCI, HIPAA, GLB, SB 1386, etc. By developing and implementing a comprehensive set of best practices that will meet the requirements of multiple regulations, the information security organization can deliver tremendous operational efficiencies to the business. The benefits of a strategic approach go way beyond compliance. With the right information security controls in place, companies and government agencies can make the most of their Internet investments and do even more online.

WHITE PAPER

RSA SECURITY® | Confidence Inspired™

THE IMPORTANCE OF BEST PRACTICES

Instead of being prescriptive, most regulations provide high-level requirements and expect organizations to implement “reasonable and appropriate measures” to protect information - in other words, information security best practices. To establish a set of best practices, organizations are advised by legislators, regulators and industry to use control frameworks and/or standards as guidance. The most cited standards include the International Standards Organization Code of Best Practices in Information Security (ISO 17799), the National Institute of Science and Technology Special Publications Series 800 (NIST 800), the Federal Financial Institutions Examination Council IT Handbook on Information Security (FFIEC) and the Control Objectives for Information Technology (COBIT).

COMMON THREADS ACROSS REGULATIONS

A strategic approach to compliance involves looking for common threads across regulatory requirements. Most regulations that mandate the protection of information, whether they are governance, privacy, or critical infrastructure regulations, all share common fundamental requirements to verify identities, allow only authorized access to information, and provide reliable audit reports. These common elements include risk management, authentication, access control, data protection and logging and reporting - the essence of identity and access management (I&AM). From an information security perspective, many organizations are focusing on I&AM in order to meet these central requirements of the regulations.

LAYERS OF PROTECTION IN IDENTITY AND ACCESS MANAGEMENT (I&AM)

To help organizations take a strategic approach to compliance, RSA Security has developed the RSA Security Best Practices Framework. It was designed specifically with regulatory compliance in mind and was derived by extracting the key I&AM-related controls from ISO 17799, NIST 800-53, FFIEC, and COBIT. The controls were then brought up to date with insights from the SANS Institute, industry analysts, and RSA Security's experience working with over 20,000 customers worldwide. This exclusive set of some 60 best practices is organized in a framework called “Layers of Protection in Identity and Access Management (I&AM)” that consists of five main categories, as illustrated in Table 1.

LAYERS OF PROTECTION IN IDENTITY AND ACCESS MANAGEMENT (I&AM)

BEST PRACTICES CATEGORY	SUBCATEGORY
RISK MANAGEMENT	Policy
	Process
AUTHENTICATION	Policy & Process
	Authentication Methods
	Log-on Procedures
ACCESS CONTROL	Policy & Process
	User & Account Management
	Rights Management & Enforcement
DATA PROTECTION	Policy & Process
	Encryption & Data Integrity
	Application Development
LOGGING AND REPORTING	Policy & Process
	Data Collection & Review

TABLE 1: The RSA Security Best Practices Framework, “Layers of Protection in I&AM,” is organized into five main categories.

SUMMARY OF THE FRAMEWORK

I. Risk Management: Best practices for developing a formalized process to identify measure, manage, and control the risks to information. These best practices include assessing risk, setting policy, developing a plan, and implementing and evaluating controls.

II. Authentication: Best practices pertaining to verifying the identity of an entity (person, device or application) based on the presentation of unique credentials to the system. Examples of authentication methods are passwords, tokens, and certificates. Authentication that relies on more than one form of credential to identify a user is called multi-factor authentication and is generally stronger than any single-factor authentication method. These best practices also cover controls used to ensure secure log-on to applications or systems.

III. Access Control: Best practices related to managing users and their access rights and allowing only authorized users to access resources. These best practices also cover developing and enforcing policy regarding what users can access and which specific actions are allowed based on business rules.

IV. Data Protection: Best practices that involve the use of cryptographic mechanisms to control access to data and protect data confidentiality and integrity. These best practices also cover technical measures for non-repudiation (so users cannot disavow their actions) and for detecting access and modifications to data.

V. Logging and Reporting: Best practices concerning the collection and presentation of logs from various applications and systems, which are used to monitor user activity, administrator actions, and security events and provide evidence of conformance to policy.

USING THE FRAMEWORK

Organizations can use the RSA Security Best Practices Framework as a starting point to establish their own set of information security best practices. As with any control framework or standard, it is intended to be tailored to an individual organization and their particular environment, objectives, and industry. In some cases, an organization will have already established their own set of best practices and may find that the RSA Security framework easily maps to their own framework. In this case, it can be used to augment or validate their best practices. Whatever stage an organization is at, most will find the RSA Best Practices Framework to be a valuable reference set of controls and an excellent "checklist" that can help to identify key competency gaps.

REGULATORY LANDSCAPE

This best practices framework was designed to help comply with regulations that mandate the protection of information such as:

- US - SARBANES-OXLEY ACT (SOX)
- UK - TURNBULL GUIDANCE
- NORTH AMERICA - NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL CYBER SECURITY STANDARDS (NERC)
- US - FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)
- US - TITLE 21 OF THE CODE FEDERAL REGULATIONS PART 11 (21 CFR PART 11)
- EU - GOOD MANUFACTURING PRACTICES ANNEX 11 (ANNEX 11)
- US - GRAMM-LEACH-BLILEY (GLB)
- US - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
- EU - DATA PROTECTION DIRECTIVE (DPD)
- JAPAN - PERSONAL INFORMATION PROTECTION ACT (PIPA)
- CALIFORNIA - ASSEMBLY BILL 1950 (AB 1950)
- AUSTRALIA - FEDERAL PRIVACY ACT (FPA)
- CANADA - PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)
- CALIFORNIA - INFORMATION PRACTICE ACT OR SENATE BILL 1386 (SB 1386) AND OTHER STATE NOTIFICATION LAWS
- GLOBAL - PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI)

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

RISK MANAGEMENT

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Policy	RM 1	Develop a Comprehensive Information Security Policy	Develop, document, and enforce an information security policy that provides management direction, support, and objectives for the information security program. The policy should cover the organization's commitment and approach to information security, the scope, goals, principles, and requirements, the roles and responsibilities, and the consequences of violations such as sanctions. Supporting policies include: data classification, authentication policy (including password policy), access control policy (including access rights based on least privilege), acceptable use policy (AUP), data protection policy, logging and reporting policy, and business continuity. Information security policies should be approved by management, regularly reviewed and updated, and clearly communicated to all employees.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • GLB • HIPAA • PCI
	RM 2	Classify Data by Sensitivity and Criticality	Classify data according to sensitivity and criticality in order to ensure information assets receive an appropriate level of protection. Some information types may be strictly confidential and/or essential to the operations of the business and therefore require higher levels of protection. Examples include employee or customer non-public personal information such as financial (credit card and bank account numbers) and healthcare data, as well as proprietary information such as financial statements or intellectual property. Classifications should be established based on the potential impact of a loss of confidentiality, integrity, or availability for that information type, and on business needs for sharing or restricting information. Defining the classification for an item of information and periodically reviewing that classification should be the responsibility of the originator or designated owner. In accordance with the classification scheme, an appropriate set of procedures for information labeling and handling should be developed. As well, data classification should be referenced in other policies (such as authentication, access control and data protection policies) and applied consistently across different systems and applications.	• ISO 17799 • NIST 800-53 • COBIT • SANS • RSA Pro Services	• NERC • FISMA

** In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

RISK MANAGEMENT - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Process	RM 3	Implement a Structured Risk Management Program	Implement a structured information security risk management program that is a formalized process designed to identify, measure, manage, and control the risks to information availability, integrity, and confidentiality, and to ensure accountability for actions. The program should use a multidisciplinary approach based on a sufficient level of expertise and up-to-date practices, should be integrated into an overall enterprise risk management program, and should be thoroughly documented. The elements of the program include a risk assessment, data classification, a security policy and plan, the implementation and testing of controls, ongoing monitoring and evaluation, and regular review by senior management. Specific and careful consideration should be given to managing the risks involved in information being accessed, processed, communicated to, or managed by external parties. Agreements for the secure handling of information by external parties such as service providers and other partners should be established.	• ISO 17799 • NIST 800-53 • COBIT • SANS • Industry Analysts • RSA Pro Services	• SOX • NERC • FISMA • 21 CFR Part 11 • GLB • HIPAA • PCI
	RM 4	Implement Integrated Risk Assessment	Implement and document a risk assessment program that systematically estimates the magnitude of risks (risk analysis) and then compares the estimated risks against risk criteria and management objectives to determine the significance of the risks (risk evaluation). Risk assessment should be integrated into the overall risk management program, providing feedback and guiding decision making and priorities. Analysis includes taking an inventory of all information assets, ascertaining threats, vulnerabilities, and potential attacks, and determining the probabilities of occurrence and possible outcomes. Evaluation is based on the organization's criteria for determining acceptable levels of risk. A risk may be accepted, for example, if it is too low to significantly affect day-to-day business operations, or if the cost of controls outweighs potential losses. Risk assessment should be performed periodically and as external and internal environments change.	• ISO 17799 • NIST 800-53 •FFIEC • COBIT • SANS • Industry Analysts • RSA Pro Services	• NERC • FISMA • GLB • HIPAA • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

RISK MANAGEMENT - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Process - *continued*	RM 5	Develop a Detailed Information Security Plan	Develop, document, and implement a detailed plan for the information security program that delineates the steps involved in assessing risk, developing policy and procedures, evaluating and deploying technology, and training users. The plan should put in place layered controls in identity and access management that establish multiple control points between threats and the organization's assets.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • FISMA • GLB • HIPAA • PCI
	RM 6	Implement Appropriate Information Security Controls	Implement information security controls appropriate to risk level, including: the acquisition, implementation, and operation of technology, the assignment of duties and responsibilities to managers, employees, and other users, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • Annex 11 • GLB • HIPAA • PCI
	RM 7	Test & Verify Information Security Controls	Test information security controls using formalized, repeatable testing methodologies to assure risk is appropriately assessed and mitigated, and verify that controls are effective and performing as intended.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • GLB • HIPAA • PCI
	RM 8	Monitor & Evaluate Controls on an Ongoing Basis	Perform ongoing monitoring and evaluation of the organization's controls and that of the external parties that access, process, exchange, or manage the organization's information system. This should include continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls, and using this information to update the risk management program. Business partner agreements should contain a "right to audit" clause so that the organization can evaluate external parties' controls.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • GLB • HIPAA • PCI
	RM 9	Separate Security Administration Duties	Separate duties for security administration by establishing appropriate divisions of responsibility in order to eliminate conflicts of interest and to reduce the risk of negligent or deliberate system misuse. For example, personnel who request access to information should not be able to grant, authorize, or administer access to that information. Personnel who administer authentication or access control systems should not be able to administer audit functions.	• ISO 17799 • NIST 800-53 • COBIT • Industry Analysts • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

AUTHENTICATION

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Policy & Process	AU 1	Develop a Comprehensive Authentication Policy	Develop and document a comprehensive authentication policy that dictates the use of mechanisms to validate user identity per system and/or application. All authentication techniques used should be governed by policy (e.g., password policy, remote access policy, Certificate Policy).	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • PCI
	AU 2	Implement Appropriate Authentication Techniques	Implement authentication techniques appropriate to risk level to ensure only authorized users with validated identities gain access to resources (e.g., network, operating system or application). Consider that the strength of an authentication method is based on the number of factors it uses in verifying the user's identity. The three factors used to verify identities are: something the user knows (e.g., password or PIN), something the user has (e.g., a token or smart card) and something the user is (e.g., biometric data such as fingerprint or Iris scan). Authentication is based on a single factor or multiple factors. Combining factors increases the strength of the authentication.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • 21 CFR Part 11 • HIPAA • PCI
	AU 3	Keep Authentication Mechanisms Effective	Keep authentication mechanisms effective by ensuring passwords are changed regularly where appropriate, promptly reporting and canceling lost or stolen authenticators and preventing system access by invalid credentials.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • 21 CFR Part 11 • PCI
	AU 4	Protect Storage & Transmission of Authentication Information	Safeguard the authentication server and secure the storage and transmission of authentication information such as passwords, PINs, certificates, etc. (i.e. do not store or transmit plain text credentials)	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• HIPAA • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

AUTHENTICATION - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Policy & Process - *continued*	AU 5	Control Authentication for Access to External Systems	Control the authentication process for all user access, including not only access to internal systems but also access to external systems (inter-organization). Avoid having external organizations such as outsourced service providers or other business partners manage your users' identity information. When external organizations manage your user's identity information, the risk of a privacy breach or identity theft is increased, as is the chance that the identity information will be inaccurate or outdated, possibility allowing unauthorized access to the system by a terminated employee, for example.	• RSA Pro Services	N/A
	AU 6	Maintain Business Continuity for Authentication Services	Counteract interruptions to business activities and protect the availability and security of information by ensuring that in the event of a disaster or computer failure, authentication services can be restored in a timely manner.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	*These regulations mention general requirements for business continuity/ disaster recovery:* • NERC • FISMA • HIPAA • PCI
Authentication Methods	AU 7	Develop & Enforce a Strong Password Policy	Develop and enforce a password policy mandating the use of strong passwords, defined as: not easily guessed, not listed in dictionaries, includes a combination of letters, numbers, and special characters with no consecutive duplicates, does not contain all numeric or all alphabetical characters, an is of a length appropriate to the risk level. (Current recommendations for password length are 8 characters since attacks can easily reveal passwords less than 8 characters in length, and with increased computing power, recommended length continues to get longer.) The policy should require passwords be kept confidential, not be shared or written down, and be changed at regular intervals (current recommendations are every 30 days for sensitive systems and 90 days for others). Temporary passwords should be changed immediately upon issuance.	• ISO 17799 • NIST 800-53 • FFIEC • SANS • Industry Analysts • COBIT • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

AUTHENTICATION - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Authentication Methods - *continued*	AU 8	Use an Automated System to Manage Passwords	Use an automated system to manage passwords that provides an interactive method of enforcing user selection of strong passwords (as defined by policy), facilitates required and/or periodic password changes, enables password resets when users forget their passwords, and prevents the re-use of passwords. The system should maintain and check a record of previously-used passwords (current recommendations are to check the previous 12 month time period).	• ISO 17799 • Industry Analysts • RSA Pro Services	*These regulations have requirements for password management (not necessarily automated):* • 21 CFR Part 11 • HIPAA • PCI
	AU 9	Protect Against Social Engineering Attacks	Protect against attacks meant to discover passwords through social engineering by implementing and enforcing controls such as strong passwords and/or multi-factor authentication in combination with comprehensive user training.	• ISO 17799 • FFIEC • Industry Analysts • RSA Pro Services	N/A
	AU 10	Use Multi-factor Authentication when Strong Passwords Fail	Use multi-factor authentication when a strong password policy actually results in weakened security; for example, when users must write passwords down so they don't forget them (easily forgotten passwords also jeopardizes the timely availability of information for authorized users). Password systems must balance the password strength with the user's ability to maintain the password as a shared secret. When passwords are too complex to remember, a different authentication mechanism should be used. Consider adding a multi-factor authentication mechanism to the legacy systems and applications for which the native login procedure cannot be configured in accordance with a strong password policy.	• FFIEC • Industry Analysts • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

AUTHENTICATION - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Authentication Methods - *continued*	AU 11	Use Multi-factor Authentication for Remote Access	Use multi-factor authentication for all remote access to systems or applications, especially when using public networks, whether over the web, via a portal, through remote-access servers (RAS) or VPNs, etc. In the case of remote access, users are connecting from locations (and possibly devices) outside of the organization's control, which represents a higher risk. For example, there are no physical safeguards to verify that the user is authorized, such as requiring the user to have a building access card in order to enter the corporate facilities and gain access to the workstation. Requiring the user to provide multiple factors when accessing systems remotely is a higher assurance method of verifying their identity that is commensurate with the higher risk.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	• NERC • 21 CFR Part 11 • PCI
	AU 12	Use Multi-factor Authentication for Access to Wireless Networks	Use Multi-factor Authentication to Control Access to Wireless Networks. Additional authentication controls are needed for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.	• ISO 17799 • RSA Pro Services	• NERC • 21 CFR Part 11 • PCI
	AU 13	Use Robust Authentication Techniques for Single Sign-On	Use multi-factor authentication or ensure the use of strong passwords for single sign-on (SSO) environments that provide access to multiple applications or systems containing confidential or critical data. For SSO, where feasible, multi-factor authentication is recommended.	• ISO 17799 • FFIEC • Industry Analysts • RSA Pro Services	N/A
	AU 14	Use Multi-factor Authentication for System Administrators	Use multi-factor authentication for system administrators accessing administrative functions where possible. Verify the identity of administrators who have extensive access rights with a high degree of assurance.	• Industry Analysts • RSA Pro Services	N/A
Log-on Procedures	AU 15	Implement Secure Single Sign-On Systems	Implement single sign-on (SSO) systems where feasible so users do not have to remember multiple passwords or possess multiple authentication mechanisms. Make sure the authentication method used is of appropriate strength to account for the “keys to the kingdom” issue.	• ISO 17799 • FFIEC • SANS • Industry Analysts • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

AUTHENTICATION - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Log-on Procedures - *continued*	AU 16	Control Display of Information During Log-on	Control the display of information throughout the log-on process, including displaying a general notice warning that the system should only be accessed by authorized users. Do not provide help messages during the log-on procedure that would aid an unauthorized user, do not display system or application identifiers until after a successful logon, and do not validate the log-on information until all input data is complete. If passwords or codes are used for authentication, do not display the characters as they are entered. Upon completion of a successful log-on, the system should display the date and time of the previous successful log-on as well as the details of any unsuccessful log-on attempts since the last successful log-on.	• ISO 17799 • NIST 800-53 • RSA Pro Services	• NERC
	AU 17	Terminate Log-on Procedure after Unsuccessful Attempts	Terminate the log-on procedure after an appropriate number of unsuccessful log-on attempts as defined in the authentication policy (current recommendations are three). Any further attempts to logon should be rejected unless specific authorization is obtained. When the maximum number of logon attempts is reached, an alarm message should be sent to the system administrator. The log-on procedure should have a minimum and maximum time allowed. If exceeded, the system should terminate the log-on.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• PCI
	AU 18	Implement Session Time-Out After Inactivity	Implement session time-out such that after a period of inactivity the network and/or application session is closed down (or at a minimum, the screen is cleared) and the user is required to re-authenticate. Time-out guards against attacks that use an unattended logged-in workstation to gain unauthorized access. The time-out delay should reflect the security risks of the physical area, the applications, and the sensitivity of information.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• 21 CFR Part 11 • HIPAA • PCI
	AU 19	Set up Emergency Access Procedures	Set up emergency access procedures to provide timely access to resources when users forget their passwords or are not in possession of their authenticators. Use a technique that can confirm the user's identity with a high level of assurance. Automated mechanisms should be used to facilitate emergency access.	• RSA Pro Services	• HIPAA

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

ACCESS CONTROL

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Policy & Process	AC 1	Develop a Comprehensive Access Control Policy	Develop and document a comprehensive access control policy that identifies authorized users, describes their access rights and allowable actions as well as the approval process for granting access rights. The policy should include an explanation of the formal procedures for controlling the management of user identities and allocation of access rights, should outline the roles and duties of administrators, managers, system or application owners, and users, and should describe the workflow process involved. Based on business and security requirements, the access control policy should be regularly reviewed and updated.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • HIPAA • PCI
	AC 2	Implement Appropriate Access Controls	Implement, manage, and enforce access controls appropriate to risk level that allow only authorized user access to resources (e.g., network, operating system, and application).	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • FISMA • 21 CFR Part 11 • Annex 11 • GLB • EU DPD • Japan PIPA • Australia FPA • Canada PIPEDA • HIPAA • PCI
	AC 3	Integrate Access Control with Effective Authentication	Integrate access control with effective authentication to ensure only authorized users whose identity has been validated with a high level of assurance, gain access to resources (e.g. network, operating system and application).	• ISO 17799 • FFIEC • COBIT • RSA Pro Services	N/A
	AC 4	Restrict Users' Knowledge of Unauthorized Functions	Restrict users' knowledge of application functions for which they are not authorized to perform. The user interface should not display functions that are not accessible to the user. Avoid using "grey-ed out" functions and instead configure the display to show users only the functions for which they are authorized to perform.	• ISO 17799 • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

ACCESS CONTROL - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Policy & Process - *continued*	AC 5	Maintain Business Continuity for Access Control	Counteract interruptions to business activities and protect the availability and security of information by ensuring that, in the event of a disaster or computer failure, access control services can be restored in a timely manner.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	*These regulations mention general requirements for business continuity/disaster recovery:* • NERC • FISMA • HIPAA • PCI
User & Account Management	AC 6	Assign Individuals Unique Credentials	Assign individual users and administrators unique IDs and credentials for access to resources (e.g., network, operating system and applications), in order to ensure that activities can be traced to individuals who are held responsible and accountable for their actions. Generally, the use of shared accounts should be avoided for all users, and all administrators should have individual accounts.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• NERC • 21 CFR Part 11 • HIPAA • PCI
	AC 7	Ensure Timely User Lifecycle Management	Actively manage access rights throughout all stages of the user lifecycle, including initial user registration as well as the requesting, approving, issuing, adding, deleting, or modifying of access rights and the deregistration of a user. The access rights of all employees, contractors and other external parties should be promptly removed upon termination of their employment, contract or agreement, or should be adjusted upon change with the appropriate personnel notified. Automated mechanisms should be used to facilitate lifecycle management.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • 21 CFR Part 11 • HIPAA • PCI
	AC 8	Remove Inactive or Redundant User Accounts	Check for and remove any inactive or redundant user accounts on a regular basis. Inactive accounts should be removed after an appropriate length of time. Current recommendations are after 30-60 days of inactivity. Automated mechanisms should be used to ensure that redundant accounts are not issued and to facilitate the removal of redundant accounts.	• ISO 17799 • NIST 800-53 • RSA Pro Services	• NERC • PCI
	AC 9	Monitor Guest/ Anonymous User Accounts	Monitor use of guest/anonymous accounts. These accounts should expire after a set time period. Automated mechanisms should be used to facilitate the expiry of accounts.	• NIST 800-53 • RSA Pro Services	• NERC • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

ACCESS CONTROL - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Rights Management & Enforcement	AC 10	Grant Rights Based on Least Privilege and Need to Know	Grant access rights based on the principle of least privilege so that users are provided the lowest level of rights and privileges necessary to perform their work for the minimum time required. Rights should also be allocated based on users' need to know, meaning the data must be necessary for the user to complete an assigned task. For example, a database administrator may require access to a database but does not need to know all of the information in the database and therefore should not be granted access to everything. Ensure that on an ongoing basis a user's access rights are set to the minimum required and reflect the user's current business needs.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • HIPAA (Privacy Standard) • PCI
	AC 11	Use Appropriate Granularity of Access Control	Select the granularity of access control based on the confidentiality or criticality of information. It should be possible to protect data at the system, application, file, record, or field level, if required.	• ISO 17799 • FFIEC • RSA Pro Services	N/A
	AC 12	Control Allowable Actions	Control allowable user actions, restricting not only their ability to access a resource but to perform actions such as read, write, delete a file, and/or execute a function or transaction.	• ISO 17799 • FFIEC • RSA Pro Services	N/A
	AC 13	Aggregate Access Rights into Groups and Roles	Aggregate user access rights using group profiles or roles to ease administrative burden and improve the security of managing access rights. Users should be assigned to appropriate groups or roles. Group employees with similar access requirements under a common access profile so application owners and security administrators can better assign and oversee access rights. For example, an employee performing a two-week job rotation does not need year-round access to perform both jobs. With group profiles, security administrators can quickly reassign the employee from one job to the next.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

ACCESS CONTROL - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Rights Management & Enforcement-*continued*	AC 14	Enforce Segregation of Duties	Enforce segregation of duties through assigned access rights in order to prevent users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. One of the key areas is to separate the initiation of an event from its approval; for example, initiating a PO and approving a PO. For financial systems, it is important to separate access to assets from responsibility for maintaining the accountability for those assets. Using automated access control and role-based access control systems can facilitate segregation of duties.	• ISO 17799 • NIST 800-53 • COBIT • Industry Analysts • RSA Pro Services	• GLB • PCI
	AC 15	Restrict System Administrator Privileges	Restrict use of system administrator privileges allowing configuration or override of access controls to a limited number of authorized administrators with the appropriate screening, training, and business need.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• NERC • PCI
	AC 16	Use Time-of-Day Limitations	Use time-of-day limitations where appropriate and feasible for applications containing sensitive information or for more sensitive application functions. This could include monitoring the number of times an account is accessed within a period of time (e.g. outside regular hours) in order to ensure accounts are not being inappropriately accessed.	• FFIEC • RSA Pro Services	N/A
	AC 17	Implement an Approval Process for Access Rights	Implement a formal approval process for assigning and updating access rights and maintain a record of all access rights and privileges allocated and authorized. All access or change requests, whether initiated by administrators or users or automatically by an information system (such as an HR system), should be subject to an approval process before access is granted. Any allocation of access rights to external parties (such as suppliers, service providers, contractors, etc.) should be especially scrutinized and subject to approvals. The process should allow for delegated authority in cases where approving personnel are absent and should ensure thorough logging of authorizations. Automated mechanisms for providing approval should be provided to support personnel including business line managers, supervisors, or application owners.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • 21 CFR Part 11 • HIPAA • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

ACCESS CONTROL - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Rights Management & Enforcement - *continued*	AC 18	Conduct Regular Reviews of Access Rights	Conduct a formal review of access rights granted to each user on the system at regular intervals to ensure access rights conform to policy, are configured accurately, and are kept current. For these reviews, the administrators and/or auditors should generate comprehensive reports on who has access to what and should distribute these to the business line managers, supervisors and/or application owners to receive their confirmation that only authorized users have access. Review periods of every 3 - 6 months are recommended. Automated mechanisms including report generation tools should be used to facilitate the review process.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • HIPAA • PCI
	AC 19	Maintain Consistent Management & Enforcement of Access Rights	Maintain consistent processes for managing access rights and enforcing policy across all systems and applications within the organization. Centralize the management and enforcement of access rights as much as possible to facilitate the use of consistent processes and help ensure access rights accuracy across multiple systems or applications.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

DATA PROTECTION

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Policy & Process	DP 1	Develop a Comprehensive Data Protection Policy	Develop and document a comprehensive data protection policy indicating when cryptographic protection is required for certain categories of data and setting the appropriate level of protection based on an organization's risk assessment and legislative and regulatory requirements. The policy should describe the specific cryptographic techniques (i.e. encryption and/or digital signatures) used to meet confidentiality, integrity and/or non-repudiation requirements. The policy should describe the type, strength, and quality of encryption algorithm and cover key management and protection.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• PCI • California SB 1386 (i.e. This and most of the other state laws, requiring notification of individuals when their data is breached, provide an exemption for data that has been encrypted.)
	DP 2	Implement Appropriate Data Protection	Use encryption for protecting data in transit or in storage commensurate with the risk level, sensitivity and criticality of data. It is recommended that encryption should always be used for sensitive data in transit and for sensitive data in storage when other access controls are not sufficient. As well, encryption should be used when data is subject to physical loss or interception to control administrator access to data (such that the administrator can work with files but not view the data) and to meet specific regulatory, privacy, or legal obligations.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	• 21 CFR Part 11 • GLB • HIPAA • PCI • California SB 1386 (i.e. This and most of the other state laws, requiring notification of individuals when their data is breached, provide an exemption for data that has been encrypted.)
	DP 3	Employ Secure Key Management Procedures	Use secure key management for symmetric and asymmetric cryptographic solutions, including logical and physical controls to safeguard the generation, distribution, and storage of keys and to protect the keys from loss, destruction, modification, or tampering. Keys should be deactivated immediately upon compromise or when they are no longer needed. A key backup and recovery system should be used to facilitate key recovery in case of loss, damage or compromise and to provide for the long-term storage and secure, timely retrieval of keys for decrypting encrypted information if required.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

DATA PROTECTION - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Policy & Process-*continued*	DP 4	Employ Stringent Root-Key Protection Measures	Employ stringent measures to safeguard critical data protection keys, such as PKI root CA keys, through mechanisms such as tamper-resistant security modules. Use strong protection procedures, such as dual control over private signing keys, as well as storing original and back-up keys on computers that do not connect with an outside network.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	N/A
	DP 5	Maintain Business Continuity for Data Protection Services	Counteract interruptions to business activities and protect the availability and security of information by ensuring that in the event of a disaster or computer failure data protection services can be restored in a timely manner.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	*These regulations mention general requirements for business continuity/disaster recovery:* • NERC • FISMA • HIPAA • PCI
Encryption & Data Integrity	DP 6	Use Encryption to Protect Data in Transit	Protect confidentiality of electronic communications with encryption when there is the risk of unauthorized access especially when sensitive information is transmitted over a public network (e.g., the Internet, email or a web session). For example, systems transmitting nonpublic personal information such as names, addresses, credit card, and other financial and health information should use such protection.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• 21 CFR Part 11 • GLB • HIPAA • PCI • California SB 1386 (i.e. This and most of the other state laws, requiring notification of individuals when their data is breached, provide an exemption for data that has been encrypted.)
	DP 7	Use Encryption to Protect Stored Data	Protect confidentiality of electronically stored data with encryption when data is at risk of unauthorized access, especially for databases accessible over the Internet. For example, consider encryption for employee or customer non-public personal information such as financial (credit card and bank account numbers) and healthcare data as well as proprietary information such as financial statements or intellectual property.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	• 21 CFR Part 11 • GLB • HIPAA • PCI • California SB 1386 (i.e. This and most of the other state laws, requiring notification of individuals when their data is breached, provide an exemption for data that has been encrypted.)

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

DATA PROTECTION - *continued*					
SUB-CATEGORY	**BP#**	**BEST PRACTICE**	**BEST PRACTICE DESCRIPTION**	**SOURCES**	**REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA***
Encryption & Data Integrity-*continued*	DP 8	Protect Data Integrity with Cryptographic Mechanisms	Protect the integrity of sensitive or critical information in transit or at rest with cryptographic mechanisms, such as hashes and digital signatures. Systems that handle sensitive ecommerce transactions or email communications should use such protection, particularly where non-repudiation capabilities are needed.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• 21 CFR Part 11
	DP 9	Implement Encryption for Wireless Systems	Protect wireless devices, communications, and systems with encryption to guard against unauthorized access or disclosure of information stored, processed, transmitted or received by these devices.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	• PCI
Application Development	DP 10	Ensure Applications Developed with Appropriate Security Controls	Ensure that applications are developed with appropriate security controls, including defining the security requirements before developing new applications, incorporating widely recognized security standards, integrating additional authentication and encryption controls where required to ensure integrity and confidentiality of the data and non-repudiation of transactions, implementing an effective change control process, hardening systems before deployment, and establishing an effective patch process for new security vulnerabilities.	• ISO 17799 • FFIEC • RSA Pro Services	• PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

LOGGING & REPORTING

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Policy & Process	LR 1	Develop a Comprehensive Logging & Reporting Policy	Develop and document a comprehensive logging and reporting policy that defines which events are logged, which activities are monitored, which reports are generated, and how long records are retained in accordance with the risk assessment. Logs and reports should be produced to meet auditing and administrative requirements, including: detecting unauthorized access or actions, uncovering indications of inappropriate or unusual activity, checking the effectiveness of controls, determining conformance to policy, and providing evidence in the case of security incidents. The policy should indicate frequency of logging certain events or activities (e.g. periodic, continuous, in response to specific situations, etc.). A reporting process should be defined that includes the content of reports as well as how often they are generated and for what purposes. Regular reviews/analysis of audit records should be conducted and delineated in the policy.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	• NERC • HIPAA • PCI
	LR 2	Protect Logging Mechanisms from Deactivation or Compromise	Protect logging mechanisms by preventing deactivation, ensuring that log files cannot be edited or deleted, protecting log files in storage and transmission, providing adequate storage capacity to avoid gaps in data gathering, safeguarding backup and disposal of log files, and logging data to a separate, isolated computer and to write-only media.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	N/A
	LR 3	Maintain Business Continuity for Logging Services	Counteract interruptions to business activities and protect the availability and security of information by ensuring that in the event of a disaster or computer failure the logging services can be restored in a timely manner.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • RSA Pro Services	*These regulations mention general requirements for business continuity/disaster recovery:* • NERC • FISMA • HIPAA • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

LOGGING & REPORTING - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIREMENTS IN THIS AREA*
Data Collection & Review	LR 4	Ensure Sufficient Data Logging	Ensure sufficient data is collected in audit log files to satisfy the objectives laid out in the policy (e.g. to investigate suspicious activity, to identify and respond to unauthorized access attempts, etc.). The kind of events and activities logged and the frequency of logging should be commensurate with risk, considering the sensitivity and criticality of the information. At a minimum, logged data should include access logs such as operating system access (especially high-level administrative or root access), application access (especially users with write- and execute privileges), remote access activities, and all unsuccessful attempts at system or application access. All administrator and operator activities and use of high-level privileges should be logged, such as changes to system or application configuration or changes to access rights and use of system utilities. Activation or deactivation of control systems should be logged and an alarm message sent to administrators. All alarms raised by the access controls should also be logged. All event and activity logs should include date and time stamps.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • HIPAA • PCI
	LR 5	Ensure Logged Data are Accessible and Reviewed Regularly	Ensure logged data is accessible and can be readily reviewed and analyzed through file interrogation and reporting tools. Logs and reports on administrator and user access and activity and security events should be reviewed regularly. Consider the use of pre-structured and automated reporting tools to facilitate report generation and review of logs.	• ISO 17799 • NIST 800-53 • FFIEC • COBIT • Industry Analysts • RSA Pro Services	• NERC • HIPAA • PCI

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

RSA SECURITY BEST PRACTICES FRAMEWORK: LAYERS OF PROTECTION IN I&AM

LOGGING & REPORTING - *continued*

SUB-CATEGORY	BP#	BEST PRACTICE	BEST PRACTICE DESCRIPTION	SOURCES	REGULATIONS WITH SPECIFIC REQUIRE-MENTS IN THIS AREA*
Data Collection & Review-*continued*	LR 6	Capture User Activity Information	Capture detailed information on the user and their activities. Depending on the policy, audit logs on user activity should include data such as user ID, session ID, terminal ID, as well as the date, time, and type of access attempt, service request, process, transaction, or functions performed or rejected (such as read, write, modify, delete). At a minimum, all rejected system, application, file, or data access attempts and other failed actions should be logged. Monitoring user activity must consider any relevant privacy regulations.	• ISO 17799 • NIST 800-53 • FFIEC • RSA Pro Services	• NERC • HIPAA • PCI
	LR 7	Utilize Centralized Logging	Utilize centralized logging and synchronized time stamps to ensure consistency and accuracy in logging across multiple systems or applications and to expedite review and analysis.	• ISO 17799 • NIST 800-53 • FFIEC • Industry Analysts • RSA Pro Services	• PCI
	LR 8	Record Significant Key Events	Record, in a secure audit log, all significant events performed with the data protection keys, including key generation, key archival, and key revocation, where each entry is time/date stamped and signed.	• ISO 17799 • FFIEC • RSA Pro Services	N/A

* *In general, regulations do not mention specific requirements but rather expect organizations to implement best practices. In some cases, regulations will get specific about certain aspects.*

IMPLEMENTING BEST PRACTICES WITH RSA SECURITY I&AM SOLUTIONS

More and more regulations continue to have major implications for information security. RSA Security helps organizations with this challenge by providing a set of useful best practices in information security and leading I&AM solutions that can be used to implement best practices.

FOR IMPLEMENTING BEST PRACTICES IN:	RSA SECURITY I&AM SOLUTIONS
RISK MANAGEMENT	RSA® Professional Services or strategic partners
AUTHENTICATION	RSA SecurID® two factor authentication RSA Digital Certificate Management solutions RSA Sign-on Manager® solution (enterprise SSO) RSA ClearTrust® solution (web SSO) RSA Federated Identity Manager solution (multi-domain SSO)
ACCESS CONTROL	RSA ClearTrust® web access management solution RSA Federated Identity Manager solution RSA Secured® partners' provisioning solutions
DATA PROTECTION	RSA BSAFE® encryption solutions RSA BSAFE® Data Security Manager solution RSA Key Manager solution
LOGGING AND REPORTING	All RSA Security solutions

ABOUT RSA SECURITY

RSA Security Inc. is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the company leads the way in strong authentication and encryption, bringing trust to millions of user identities and the transactions that they perform. RSA Security's portfolio of award-winning identity & access management solutions helps businesses to establish who's who online - and what they can do. With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve more than 20,000 customers around the globe and interoperate with more than 1,000 technology and integration partners. For more information, please visit www.rsasecurity.com.

CBP WP 0406

RSA SECURITY®

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie