SRA International
Managed Information Systems
Internal Audit Report

Report #2014-03

June 18, 2014

CANCER PREVENTION AND RESEARCH INSTITUTE OF TEXAS

Table of Contents

Executive Summary

In response to two findings from the State Auditor's Report, Internal Audit has been asked to perform a review of two proprietary information systems operated by SRA International, Inc.'s (SRA), the third-party vendor under contract with CPRIT to provide pre- and post-award grants management services. These information systems allow applicants to submit grant applications, peer reviewers to submit application critiques and scores, grantees to submit financial and progress reports, and CPRIT to track, monitor, and maintain all grantee reports.

An internal audit was conducted in May 2014 to understand internal controls at SRA as they relate to the American Institute of Certified Public Accountants (AICPA) Trust Service Principles. The review was performed using the AICPA Guide: *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* focusing on the following trust principles:

- Common Criteria
  - Organization and Management
  - Communications
  - Risk Management and Design and Implementation of Controls
  - Monitoring of Controls
  - Logical and Physical Access Controls
  - System Operations
  - Change Management
- Processing Integrity

During the internal audit of SRA, no findings or observations were noted that would significantly impact the processing capability of SRA's applications, as related to services provided to CPRIT. While no significant findings were noted during this audit, CPRIT should continue to require SRA to validate their control environment and re-perform this audit periodically.

It is not feasible for all of the control objectives relating to the processing of data to be completely achieved through SRA's implemented controls. While SRA achieves some objectives, procedures performed by CPRIT contribute significantly to the overall achievement of control objectives. See section "CPRIT Control Responsibilities" for more details around CPRIT's responsibilities.

Background Information

Background

Texas voters approved a constitutional amendment in 2007 establishing the Cancer Prevention and Research Institute of Texas (CPRIT) and authorized the state to issue $3 billion in bonds to fund groundbreaking cancer research and prevention programs and services in Texas. To date, CPRIT has funded over 500 grants totaling over $1 billion.

CPRIT's goals are to:

- Create and expedite innovation in the area of cancer research, thereby enhancing the potential for a medical or scientific breakthrough in the prevention of cancer and cures for cancer;
- Attract, create, or expand research capabilities of public or private institutions of higher education and other public or private entities that will promote a substantial increase in cancer research and in the creation of high-quality new jobs in this State; and
- Continue to develop and implement the Texas Cancer Plan by promoting the development and coordination of effective and efficient statewide public and private policies, programs, and services related to cancer and by encouraging cooperative, comprehensive, and complementary planning among the public, private, and volunteer sectors involved in cancer prevention, detection, treatment, and research.

Applications for grants are submitted through the CPRIT Application Receipt System (CARS), an online application receipt system that is managed by SRA International, Inc. Peer reviewers utilized the Program and Peer Review Management Information System (P^2RMIS), an online portal that supports grant evaluation activities. Once applications are approved as grant awards and move towards the executed contract stage, CPRIT's grants management system, CGMS, which is a customization on the CARS information system platform tracks the contract, correspondence, and other compliance documentation for each grant. CGMS was put into production on October 4, 2012. Additional functionality will continue to be developed on an as needed basis. Refer to Appendix A for an illustration of the SRA enabled processes.

Audit Objectives

Our overall objectives of the internal audit were to:

- Understand the policies and procedures in place at SRA
- Understand the control activities in place at SRA
- Map the control activities to the relevant trust principle and determine whether these are sufficient to address the relevant trust principle
- Test the control activities for design effectiveness.
- Identify any gaps or deficiencies.

The policies and procedures reviewed and the testing performed focused on SRA's environment as it relates to services provided to CPRIT.

Scope

The audit performed was designed to evaluate compliance with the relevant trust service principles established by the AICPA. The two principles that this audit focused on are Common Criteria and Processing Integrity. Internal Audit interviewed SRA staff and completed testing on the identified control activities as of May 2014.

Testing Approach

To accomplish the audit objectives, Internal Audit focused on the following areas:

- **Organization Management**
  - Defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system enabling it to meet its commitments and requirements as they relate to security, availability and processing integrity
  - Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated
  - Personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system have the qualifications and resources to fulfill their responsibilities
  - The entity has established employee conduct standards, implemented employee candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and processing integrity

- **Communications**
  - Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation
  - The entity's commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities
  - Internal and external system users have been provided with information on how to report security, availability and processing integrity failures, incidents, concerns, and other complaints to appropriate personnel

- **Risk Management and Design and Implementation of Controls**
  - The entity (1) identifies potential threats that would impair system security, availability and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies)
  - The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy
  - The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly impact the system of internal control for security, availability and processing integrity and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of

control activities based on the operation and monitoring of those activities, and updates them as necessary

- **Monitoring of Controls**
  - The design and operating effectiveness of controls are periodically evaluated against security, availability, confidentiality and processing integrity commitments and requirements

- **Logical and Physical Access Controls**
  - Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access
  - Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel
  - The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, confidentiality and processing integrity

- **System Operations**
  - Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.
  - Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures

- **Change Management**
  - Security, availability, and process integrity commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.
  - Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and processing integrity commitments and requirements

Testing Methodology

In order to meet the objectives stated above, Internal Audit conducted interviews, evaluated controls and reviewed selected policies and procedures. Judgmental sampling was used to improve the overall efficiency of the assessment.

Our procedures included discussions with the following SRA personnel:

Name	Title
Jennifer Boothe	SRA – Project Manager
Karen Wan	SRA – Product Owner and Technical Manager
Mike Wingo	SRA – IT Manager

Statement of Auditing Standards

This assessment was conducted in accordance with AICPA Guide: *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. The internal audit also follows the guidelines set forth by the Institute of Internal Auditors (IIA) and conforms to the Standards for the Professional Practice of Internal Auditing, the code of ethics contained in the Professional Practices Framework as promulgated by the IIA. Grant Thornton was not engaged to perform audit or attest services under AICPA auditing or attestation standards or to provide any form of attest report or opinion under such standards in conjunction with this engagement.

Although due professional care in the performance of this audit was exercised, this should not be construed to imply that unreported irregularities to not exist. The deterrence of fraud is the responsibility of management. Audit procedures alone, even when executed with professional care, do not guarantee that fraud will be detected.

Observations and Recommendations

AICPA Trust Service Principles Criteria, Control Activities, and Testing Results

This section presents the specific control activities specified by SRA to achieve the trust principle criteria. Our review addressed controls pertaining to the following scope areas:

Common Criteria

- Organization and Management
- Communications
- Risk Management and Implementation of Controls
- Monitoring
- Logical and Physical Access
- System Operations
- Change Management

Processing Integrity

- Data Processing
- Data Retention

Also, included in this section is the following information:

- A description of the testing performed by the Internal Audit to determine whether SRA's controls were operating with sufficient effectiveness to achieve the specified criteria,
- The results of the tests of operating effectiveness and any exceptions noted.

Common Criteria – Organization and Management

AICPA Criteria	Control #	Control Activity	Testing Results
CC1.1 - The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system enabling it to meet its commitments and requirements as they relate to security, availability and processing integrity	CC1.1	SRA has established a Security policy which covers assigning responsibility for system security. The company has defined an organizational structure and posted an organizational chart to the company website. The organizational chart is reviewed and updated at least once every two years.	No exception noted.

AICPA Criteria	Control #	Control Activity	Testing Results
CC1.2 - Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated.	CC1.2	Company policies are documented, posted to the company website for employee access, and reviewed once every two years by management.	No exception noted.
CC1.3 - Personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the system affecting [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] have the qualifications and resources to fulfill their responsibilities.	CC1.3-01	Job requirements are documented in the job descriptions and are available for employee access.	No exception noted.
	CC1.3-02	The company has defined an organizational structure and posted an organizational chart to the company website. The organizational chart is reviewed and updated at least annually.	No exception noted.
	CC1.3-03	New and updated system access requests are approved by management prior to access being granted.	No exception noted.
CC1.4 - The entity has established employee conduct standards, implemented employee candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and processing integrity.	CC1.4-01	SRA has established a Background Check Policy for all the employees.	No exception noted.
	CC1.4-02	All employees must attend annual training in order to comply with current and updated company policies relevant to their job responsibilities.	No exception noted.
	CC1.4-03	New employees sign an acknowledgement form, indicating that they have read and agree to company policies relevant to their job responsibilities.	No exception noted.

Common Criteria – Communications

AICPA Criteria	Control #	Control Activity	Testing Results
CC2.1 - Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	CC2.1	Company policies are documented, posted to the company website for employee access, and reviewed annually by management. (Refer to CC1.2)	No exception noted.
CC2.2 - The entity's commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	CC2.2-01	All employees must attend annual training in order to comply with current and updated company policies relevant to their job responsibilities. (Refer to CC1.4)	No exception noted.
	CC2.2-02	New employees sign an acknowledgement form, indicating that they have read and agree to company policies relevant to their job responsibilities. (Refer to CC1.4)	No exception noted.
CC2.5 - Internal and external system users have been provided with information on how to report security, availability and processing integrity failures, incidents, concerns, and other complaints to appropriate personnel.	CC2.5	Tracking of incidents (including complaints and disputes) and security breaches of Company policies are monitored through the JIRA ticketing system.	No exception noted.
CC2.6 - System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security, availability, and process integrity are communicated to those users in a timely manner.	CC2.6	Appropriate groups are notified prior to or within one business day of the implementation of an application change, if necessary.	No exception noted.

Common Criteria – Risk Management and Design and Implementation of Controls

AICPA Criteria	Control #	Control Activity	Testing Results
CC3.1 - The entity (1) identifies potential threats that would impair system security, availability and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	CC3.1-01	SRA has a continuous monitoring program in place to identify and minimize risks including Quarterly vulnerability scans, a patch management program and regularly scheduled re-assessment of security controls.	No exception noted.
	CC3.1-02	Network availability and capacity is monitored via monitoring tools which are configured to send alerts if a system or device reaches configured thresholds.	No exception noted.
	CC3.1-03	An intrusion prevention system is in place to monitor and prevent unauthorized access to the network and applications.	No exception noted.
	CC3.1-04	Anti-virus software is installed on employee workstations and updated on a daily basis.	No exception noted.
CC3.2 - The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	CC3.2-01	Company policies are documented, posted to a network share folder for employee access, and reviewed annually by management. (Refer to CC1.2)	No exception noted.
	CC3.2-02	The Company's Disaster Recovery and Business Continuity Plan is tested on a quarterly basis and any issues identified are documented and resolved.	No exception noted.
	CC3.2-03	SRA has a continuous monitoring program in place to identify and minimize risks including Quarterly vulnerability scans, a patch management program and regularly scheduled re-assessment of security controls. (Refer to CC3.1)	No exception noted.
CC3.3 - The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly impact the system of internal control for security, availability and processing integrity and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	CC3.3	SRA has a continuous monitoring program in place to identify and minimize risks including Quarterly vulnerability scans, a patch management program and regularly scheduled re-assessment of security controls. (Refer to CC3.1)	No exception noted.

Common Criteria – Monitoring of Controls

AICPA Criteria	Control #	Control Activity	Testing Results
CC4.1 - The design and operating effectiveness of controls are periodically evaluated against security, availability, confidentiality and processing integrity commitments and requirements.	CC4.1-01	SRA has a continuous monitoring program in place to identify and minimize risks including Quarterly vulnerability scans, a patch management program and regularly scheduled re-assessment of security controls. (Refer to CC3.1)	No exception noted.
	CC4.1-02	Network availability and capacity is monitored via monitoring tools which are configured to send alerts if a system or device reaches configured thresholds. (Refer to CC3.1)	No exception noted.
	CC4.1-03	An intrusion prevention system is in place to monitor and prevent unauthorized access to the network and applications. (Refer to CC3.1)	No exception noted.
	CC4.1-04	The Company's Disaster Recovery and Business Continuity Plan is tested on a quarterly basis and any issues identified are documented and resolved. (Refer to CC3.2)	No exception noted.

Common Criteria – Logical and Physical Access Controls

AICPA Criteria	Control #	Control Activity	Testing Results
CC5.1 - Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	CC5.1-01	SRA has established a Security Policy which covers preventing unauthorized access. A valid user ID and password is required to access the SRA applications.	No exception noted.
	CC5.1-02	Administrative access to the network is restricted to the Hosting group and administrative access to the application software is restricted to the Project team.	No exception noted.
	CC5.1-03	Password rules are configured on the network to enforce the following: 1. 8 minimum length 2. 90 day expiration 3. Complexity required	No exception noted.
	CC5.1-04	An intrusion prevention system is in place to monitor and prevent unauthorized access to the network and applications. (Refer to CC3.1)	No exception noted.
	CC5.1-05	Firewall rules are configured to restrict access to the network.	No exception noted.
CC5.2 - New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	CC5.2-01	New employee's access to the SRA applications and related databases must be approved by the project manager through the HelpDesk ticketing system JIRA to verify access is appropriate based on the user's job responsibilities.	No exception noted.
	CC5.2-02	Terminated employees' access is removed within one business day.	No exception noted.
CC5.3 - Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	CC5.3-01	A valid user ID and password is required to access the SRA applications. (Refer to CC5.1)	No exception noted.
	CC5.3-02	SRA has established a Security Policy which covers preventing unauthorized access. A valid user ID and password is required to access the SRA applications. (Refer to CC5.1)	No exception noted.

AICPA Criteria	Control #	Control Activity	Testing Results
CC5.4 - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	CC5.4-01	Administrative access to the SRA applications and related databases is appropriately restricted based on job function.	No exception noted.
	CC5.4-02	Terminated employees' access is removed within one business day. (Refer to CC5.2)	No exception noted.
	CC5.4-03	User accounts are reviewed for appropriateness by management on a semi-annual basis.	No exception noted.
CC5.5 - Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	CC5.5-01	Physical access to the data center housing SRA systems and storage devices and media is restricted to authorized individuals via key-cards, biometrics, man-traps, locked cages, camera coverage and 24X7 video monitoring.	No exception noted.
	CC5.5-02	Terminated employees' physical access is removed within one business day.	No exception noted.
	CC5.5-03	Physical access is reviewed by management on a quarterly basis.	No exception noted.
CC5.6 - Logical access security measures have been implemented to protect against unauthorized security and confidentiality threats from sources outside the boundaries of the system.	CC5.6	Firewall rules are configured to restrict access to the network. (Refer to CC5.1)	No exception noted.
CC5.8 - Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	CC5.8	Symantec is loaded on workstations and servers to help mitigate the risk of virus threats.	No exception noted.

Common Criteria – System Operations

AICPA Criteria	Control #	Control Activity	Testing Results
CC6.1 - Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	CC6.1	SRA I/T personnel performs security and vulnerability assessments quarterly.	No exception noted.
CC6.2 - Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	CC6.2	Tracking of incidents (including complaints and disputes) and security breaches of Company policies are monitored through the JIRA ticketing system. (Refer to CC2.5)	No exception noted.

Common Criteria – Change Management

AICPA Criteria	Control #	Control Activity	Testing Results
CC7.1 - Security, availability, and process integrity commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	CC7.1	A documented policy is in place that provides testing and approval requirements for change management.	No exception noted.
CC7.2 - Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality]	CC7.2	Company policies are documented, posted to the company website for employee access, and reviewed once in two years by management. (Refer to CC1.2)	No exception noted.
CC7.3 - Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	CC7.3	Change requests are sent to CPRIT and documented through the change management system.	No exception noted.
CC7.4 - Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and processing integrity commitments and requirements.	CC7.4-01	Changes must be approved and reviewed by CPRIT prior to implementation into production.	No exception noted.
	CC7.4-02	Changes are developed and tested in a segregated environment from production.	No exception noted.
	CC7.4-03	Programmers are denied access to production libraries, unless a firewall exception is obtained for temporary access.	No exception noted.
	CC7.4-04	Changes are tested prior to implementation into production.	No exception noted.
	CC7.4-05	Changes are promoted to production by authorized personnel.	No exception noted.

Processing Integrity

AICPA Criteria	Control #	Control Activity	Testing Results
PI1.1 - Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	PI1.1-01	A data retention policy is maintained and updated on an annual basis. (Refer to CC1.2)	No exception noted.
	PI1.1-02	Daily incremental and weekly full backups are performed.	No exception noted.
	PI1.1-03	A restoration test is performed on backup data on a bi-monthly basis	No exception noted.
	PI1.1-04	Backup results are monitored on a daily basis and failures or issues are resolved.	No exception noted.
PI1.4 - Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	PI1.4-01	A data retention policy is maintained and updated on an annual basis. (Refer to CC1.2)	No exception noted.
	PI1.4-02	Daily incremental and weekly full backups are performed. (Refer to PI1.1)	No exception noted.
	PI1.4-03	A restoration test is performed on backup data on a bi-monthly basis. (Refer to PI1.1)	No exception noted.
	PI1.4-04	Backup results are monitored on a daily basis and failures or issues are resolved. (Refer to PI1.1)	No exception noted.
Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	PI1.6-01	Administrative access to the network and SRA applications is restricted to personnel whose job functions require it.	No exception noted.
	PI1.6-02	User accounts are reviewed for appropriateness by management on an annual basis.	No exception noted.
	PI1.6-03	Changes are requested and documented through the change management system.	No exception noted.
	PI1.6-04	Changes must be approved by management prior to implementation into production. (Refer to CC7.4)	No exception noted.

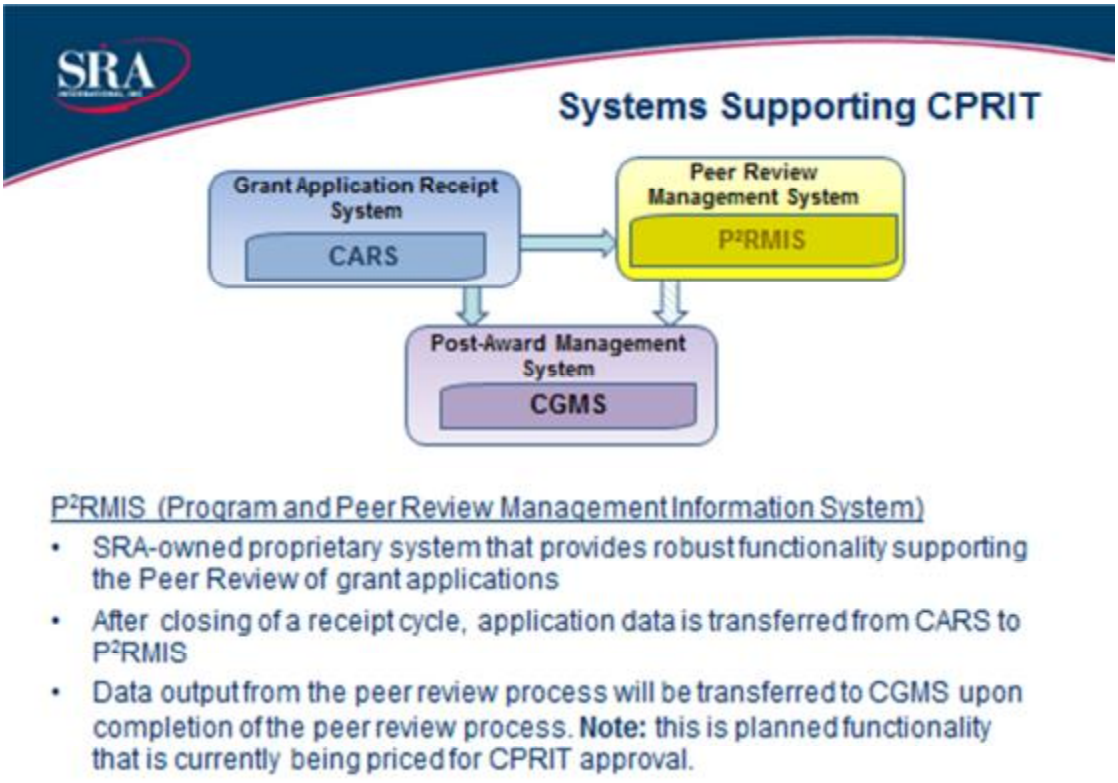
CPRIT Control Responsibilities

It is not feasible for all of the control objectives related to data processing to be achieved entirely by SRA's implemented controls. While SRA can achieve most objectives, procedures performed by CPRIT contribute significantly to the overall achievement of control objectives.

Other control objectives may be defined by and must be performed solely by CPRIT.

- CPRIT is responsible for ensuring that CPRIT specific data is complete and accurate prior to submission to SRA International.
- CPRIT notifies SRA of employee transfer activities stating what access needs to enabled or disabled.
- CPRIT has controls in place to ensure changes follow the established change management processes by approving changes to the SRA applications prior to implementation, maintaining a list of pre-approved changes and conducting periodic change controls meetings.

Appendix A: Systems Supporting CPRIT



P²RMIS (Program and Peer Review Management Information System)

- SRA-owned proprietary system that provides robust functionality supporting the Peer Review of grant applications
- After closing of a receipt cycle, application data is transferred from CARS to P²RMIS
- Data output from the peer review process will be transferred to CGMS upon completion of the peer review process. **Note:** this is planned functionality that is currently being priced for CPRIT approval.