Arizona State University
Office of University Audits
Security Incident Response Program Audit
August 10, 2018

This page left blank intentionally.

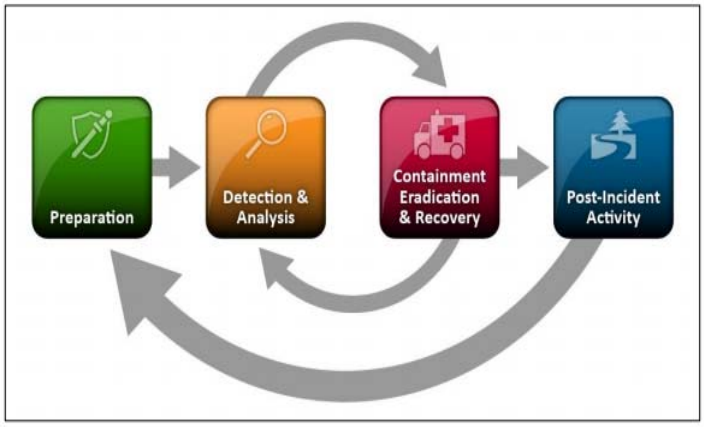
Arizona State University
Security Incident Response Program
Audit Report
August 10, 2018

Summary: The Security Incident Response Program audit was included in the Arizona State University (ASU) FY2018 audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and ASU senior leadership. The audit focused on the overall design and effectiveness of the Security Incident Response Program to ensure the protection of critical information and systems. This is the first time this area has been audited. This audit is in support of ASU's mission of preserving the availability, confidentiality and integrity of its information resources.

Background: Security incident management is the process of identifying, managing, recording and analyzing security incidents, which can come in the form of an active threat, an attempted intrusion or a successful compromise or data breach. Policy violations, unauthorized access, denial of service, compromised credentials, phishing, and malicious code are some examples of security incidents.

The Information Security Office has developed and implemented a Security Incident Response Standard and related process document to guide ASU's efforts in managing the risks associated with security incidents. The program applies to all users of ASU's computing, internet and communications resources. It also applies to all networking, computing, and data devices, both personally owned or university owned, attached to the ASU network and/or involved in storage or delivery of ASU data. The program leverages the National Institute of Standards and Technology (NIST) SP 800-61 four-phase life cycle:

Preparation: An ongoing process, which is integrated with aspects of the Information Security Program such as risk management, security configuration, monitoring, governance and policy. This provides the foundation on which all Incident Response activities are built.



Detection & Analysis: Activity that detects and triggers an incident response including initial triage, analysis, categorization and potential escalation.

Containment, Eradication & Recovery: Activities including determining appropriate containment strategy, gathering information, performing necessary eradication actions and

recovery strategies. The objective is to stop the threat from spreading, remove the threat from the affected system and restore back to a known good state.

Post-Incident Activity: Processes to review the event, complete root cause analysis, actions taken, results and mitigation strategies. In addition, this phase addresses process improvement activities including updating the defined policy and process with lessons learned.

ServiceNow, a legacy ticketing system, is utilized to report, manage and document security incidents. Custom configuration has been implemented within ServiceNow to support the defined process including automated assignment, workflow, and escalation procedures. The Information Security Office is responsible for managing incident response activities including incorporating other ASU staff as necessary based on the nature of the incident.

Audit Objectives: The objectives of the engagement were to assess the design and operating effectiveness of the ASU Information Security Incident Response Program. Specifically, the following areas were included:

- Assess the design of the Information Security Incident Response Program;
- Ensure appropriate controls are in place to detect, contain, remove and recover from security incidents;
- Assess the internal and external communication processes related to incidents;
- Assess post-incident activities;
- Assess compliance to relevant policies, laws and regulations; and
- Identify opportunities for improvement.

Scope: The scope of the audit focused on the ASU Information Security Incident Response Program for the period April 2017 through March 2018. Specifically, the audit focused on the response process from the time incidents are detected through resolution. It did not cover the various continuous monitoring processes and controls in place to monitor and identify potential security events.

Methodology: Our audit consisted of tests and procedures necessary to provide a reasonable basis for expressing our opinion. Specifically, audit work consisted of interviews with representatives of Information Security, review of documented policies and procedures, and substantive tests including the following areas:

- Evaluating the Information Security Incident Response Program design using the National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2 as a framework to ensure all required elements have been addressed.
- Reviewing the Data Handling Standard to verify that roles/responsibilities are defined and align with the incident management roles on identifying and determining if an incident has occurred.
- Confirming procedures exist and define the necessary steps for containing, removing and recovering from the security incident for each of the prioritized incident types.
- Assessing compliance to the defined incident management process by assessing a sample of 88 incidents.
    - Ensure incident was addressed in a timely manner based on the defined timeframes.
    - Ensure actions followed the defined procedures and included appropriate documentation regarding actions and resolutions.
- Confirming that appropriate notification, communication, documentation, and reporting is occurring for significant incidents to ensure timely and appropriate resolution by assessing a sample of nine significant incidents.
- Confirming post-incident activities are occurring that are focused on improving the overall effectiveness of the Security Incident Response program through inquiry with the Information Security Office and review of five weekly internal status updates.
- Confirming weekly reporting is performed to report overall security posture including general information on security incident response activities by assessing a sample of five weekly reports.
- Validating the Chief Information Security Officer meets with the InfoSec task force at least annually to discuss information security activities, including incidents, to ensure transparency and appropriate awareness. In addition, ensure that that the task force includes representation from the various functional groups across the university.

Conclusion: Overall, Information Security has developed and implemented an effective Security Incident Response Program to support the continued security of ASU services, assets and data before, during and after a security incident. The program addresses the four key phases of incident response and includes appropriate policy, procedure and work guides to support the program.

The defined process is generally being followed; however, improvement is needed to ensure that incidents are resolved or escalated within the defined timeframes, which range from four hours to one week based on the incident type. Testing indicated that 10% of the incidents reviewed (9 of 88) were not resolved and/or escalated in the required timeframe. The resolution timeframes for the exceptions ranged from three days to 79 days with most exceptions being

tied to issues with the escalation process related to ServiceNow configuration or data input errors, which resulted in escalation actions not occurring.

It was also noted that further enhancement is necessary in significant incident reporting to ensure reports are updated with final information and status. Each of the nine significant incident reports tested had one or more missing or incomplete items. Common items noted included draft status, inaccurate incident response team members, missing report components, tasks showing in outstanding status, and open recommendations that did not have formal tracking to ensure they are completed.

The control standards we considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Reliability and Integrity of Financial and Operational Information	Not Applicable	N/A	N/A
Effectiveness and Efficiency of Operations			
• Defined procedures exist for security incidents that detail the steps for containing, eradicating and recovering from the incidents.	Reasonable to Strong Controls in Place	N/A	N/A
• Incidents are resolved in a timely manner, follow the defined procedures and include appropriate documentation regarding actions and resolutions.	Opportunity for Improvement	1,2	5,6
• Management reporting is in place to ensure adequate visibility into incident management activities including trends and overall security posture and awareness.	Reasonable to Strong Controls in Place	N/A	N/A
Safeguarding of Assets			
• The Data Handling Standard appropriately covers protection of data and effectively defines requirements, roles, and responsibilities.	Reasonable to Strong Controls in Place	N/A	N/A
Compliance with Laws and Regulations			
• The ASU Security Incident Management Standard and Process Documents meet the requirements of an effective program as defined by NIST 800.	Reasonable to Strong Controls in Place	N/A	N/A

We appreciate the assistance of Information Security Office representatives during the audit.

Gordon Murphy

Gordon Murphy, CPA, CFE, CGMA
Internal Auditor Senior

Lisa Grace

Lisa Grace, CPA, CIA, CISA
Executive Director

Audit Results, Recommendations, and Responses

1. Security Incidents are not resolved or escalated within the required timeframe.

Condition: The security incident response process defines required timeframes for incidents to be resolved or escalated to ensure timely response to threats in the environment. Resolution timeframes are established by incident type and include required escalation actions if not resolved. Testing indicated that 10% of the incidents tested (9 of 88) were not resolved and/or escalated in the required timeframe. The resolution timeframes for the exceptions ranged from three days to 79 days with most exceptions being tied to issues with the escalation process related to ServiceNow configuration or data input errors, which resulted in escalation actions not occurring. In addition, two instances were noted where not all tasks were completed prior to the Information Security team closing the ticket.

Criteria: Based on the incident type, timeframes have been established using standard business days or hours ranging from four hours to one week. Escalation contacts have also been established to ensure appropriate visibility when tasks are not resolved in the expected timeframe.

Cause: Monitoring processes are not effective to identify when tasks are not resolved in a timely manner. As a result, tasks are sometimes not completed timely. In some of the issues, the escalation actions were not triggered due to data entry issues or configuration issues related to the escalation workflow.

Additionally, it was noted that ServiceNow has limited reporting capability, which further affects Information Security's ability to create standard reporting to track past due incidents or tasks.

Effect: Information Security is not aware that tasks are past due resulting in issues not being resolved timely.

Recommendation: Create reporting that tracks incidents and tasks that are past due. Utilize the reports to implement additional performance metrics around timeliness to determine if additional process improvements are required to ensure timely resolution.

In addition, review should be performed within ServiceNow to ensure escalation logic is appropriate for all incident types.

Management Response: The Incident Response Team has enhanced the weekly review process to ensure that all incidents are closed timely and appropriate action is taken to escalate, if necessary. This was implemented in August 2018. The Information Security Team is also investigating the Security Module of ServiceNow, which provides stronger and more streamlined reporting and escalation processes.

2. Significant incident reporting should be enhanced to ensure reports are complete and accurate.

Condition: Each of the nine significant incident reports tested had one or more missing or incomplete items even through the incident was considered closed. Common items noted included draft status, inaccurate Incident Response Team members, missing report components, tasks showing in outstanding status, and open recommendations that do not have formal tracking to ensure they are completed.

In addition, there currently is not a defined definition of what constitutes a significant event.

Criteria: A standard reporting template has been implemented to document significant incidents. The report includes the following data elements: executive summary, level of incident, data involved/notification required, impact to business, actions taken, recommendations, incident response team information, type of incident, data description, data owner, incident timeline and action items.

Cause: The standard report templates are being utilized and are updated throughout the incident as information is collected and actions are performed; however, once the incident has been resolved, appropriate follow up is not performed to ensure final information is captured in the report and issued as final.

Effect: Documentation for significant incidents is missing key information, contains incorrect information or reflects open action items. In addition, remediation strategies for future events or lessons learned may be lost instead of being utilized to improve the overall effectiveness of the incident management program.

Recommendation: Formalize the significant incident procedures within the existing process document. Procedures should include defined guidelines of what constitutes a significant

incident, required reporting elements and format and a formal review process once the incident is resolved to ensure final actions and status are appropriately reflected in the report.

It is also recommended that the report template be updated to include the final close date of the incident.

Management Response: The Incident Response Team will expand the existing procedure document to define what constitutes a significant incident and to clearly define the additional requirements that must be completed. A final close date has been added to the template. All identified reports have been reviewed and updated. The procedure updates will be completed in August 2018.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Lev Gonick, Chief Information Officer
Tina Thorstenson, Deputy Chief Information Officer and Chief Information Security Officer
Evelyn Pidgeon, Director Information Security
Internal Audit Review Board