Audit Plan for Security Response Policy

Introduction

I would like to thank JMTSJ University for offering Parallax Consultants the opportunity to audit your IT security response policy. Allowing our team to audit your policy will strengthen your compliances as well as the message that you are sending to your audience. We believe in taking lessons learned in current crises and from existing models and implementing safeguards that make sense to promote a stronger policy.

Audit Team

Our Auditing team will be responsible for overseeing the audit including planning, testing and reporting. Our Audit team will deliver an overall scorecard based on best practices and other external audits that have been published and will make recommendations from the audit. These audits will provide a baseline for future audits that will strengthen your policies and will add value to your policies while making your environment safer.

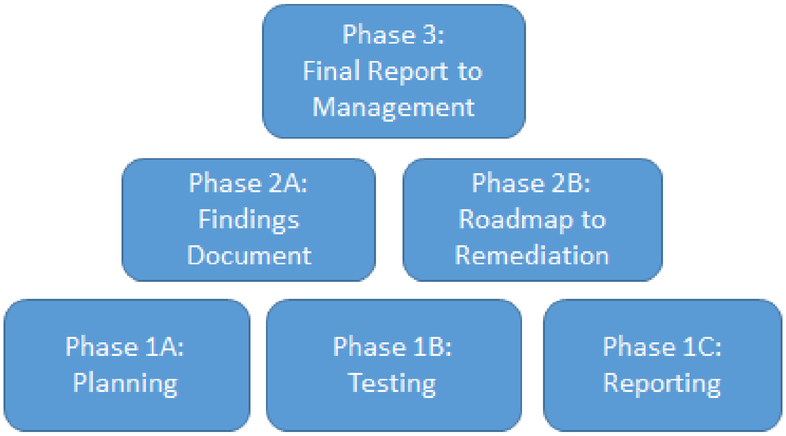
Audit Team Members:

Tamer Tayea - Information Risk Analysis
Jon Whitehurst - Network Infrastructure
Joshua Zenker - PCI and Compliance
Mushima Ngalande - Data Privacy
Shain Amzovski - Attack and Penetration Testing

Audit Process

Our phased approach of planning, testing, and reports on evidence will provide deliverable documents based on the testing, a findings document, a roadmap for remediation and a final report. The final report will be your building block to the policy and grow to become more efficient as time goes on.

Parallax Phased Audit Plan For 2015:



Time

Depending on the Statement of Work and complexity of the policy this approach can take from three to six weeks to present a final report. The remediation depending on our findings can take between one to three months before the findings can be corrected. After remediation, your policy will be running more efficient while adding value.

Scope

The audit shall cover the policy objectives of Documentation, Reporting, Classification and Triage, Communication, Incident Management, Roles and Responsibilities, and Training.

Objectives

The audit will evaluate whether this policy provides appropriate guidelines that ensure that security incidents are reported, identified, prioritized, investigated, and remediated in a timely and consistent manner.

Secondly the audit is to investigate whether there is an incident communication procedure and a governance framework.

Lastly the audit will identify whether responsibility has been assigned to people and also if there is accountability in the process of addressing security incidents.

Policy Category	Control Objectives	Control Activities	Test Procedures	Evidence
1. Documentation	Ensure IT security incident response policy is formally documented and updated periodically.	Formal documentation of the policy with input from stakeholders and approved by Board of Trustees.	Review Recent copy of Information Security Response Policy and look under table of revisions to show how many revisions have been done in the last year.	Information Security Response Policy document.
		Review and updating of the policy every 6 months or whenever there is a security risk with final approval from CISO		Change log
		Office of CISO is to Communicate policy to all employees who have to agree to terms of policy.		Copy of communications.
	Identify and clarity ownership of policy	Information Security Team, which includes management level and technical staff are assigned ownership of Policy.	Review Percentage of employees and users who can correctly name the policy's owner	Record of the policy's owner
		Communication of policy ownership		
2. Reporting	Ensure that users report incidents through the right channels and in a timely manner	End Users are to report security related events directly to the Help Desk	Obtain sample of all reported incidents and ensure that the Help Desk obtained all relevant information and followed the policy from the time event was reported.	Tickets of incidences from JMTSJ web portal with documentation of escalation, which include detailed description, employee signature, and supervisor signature.
				Incident report forms
				Published information on how the Help Desk/Office of the CISO spread awareness of the reporting process to students, administrative staff and faculty
				Report on skill proficiency matrix of Help Desk staff
		Computer Services staff are to report suspicious activities to immediate supervisors	Obtain sample of all reported incidents then categorize incidents into end users and computer services staff then check that computer services staff followed the policy from the time event was reported.	Tickets of incidences with documentation of escalation, which include detailed description, employee signature, and supervisor signature.
				Staff incident report forms

		The Office of the CISO are to report the event to upper management and law enforcement	Obtain sample of reported incidents from the Computer Services category and check that office of CISO followed the policy from the time event was reported.	Tickets of incidences with documentation of escalation, which include detailed description, employee signature, and supervisor signature.
			Review crime logs.	Security Reports and Crime logs from Campus Safety Department.
		Ensure incidents have received the appropriate attention within initial time frames.	Review incidents that were not resolved in a timely manner. This requires review of sample tickets obtained earlier to check if the Help Desk has a "max resolution time limit" after which the incident is referred to 3rd level support within the Help Desk and/or to another Computer Services group for further investigation.	Tickets of incidences with documentation of escalation, which include detailed description, employee signature, and supervisor signature.
3. Classification and Triage	Ensure that all reported incidents are evaluated, categorized, classified, and prioritized.	Office of CISO are to assign a severity rating of high, medium or low to an incident.	Review sample tickets obtained for proper severity assignment given ticket details of impact analysis, threat evaluation, and quantification. Exceptions will be noted where severity assignment process did not follow policy guidelines.	Tickets of incidences from JMTSJ web portal.
			High - Incident Rating:	
			Review reports of network downtime due to DDoS Attack	Network Firewall System security logs
			Review reports in which a critical University system was unavailable due to a security breach	Security and crime logs from campus safety
			Review incidents in which an active virus with no known signature spread through the compute environment	Intrusion Detection System (IDS) logs
			Review incidents in which there was a security breach of financial data, research materials, or NPI of the University, its students, or its employees	
			Medium - Incident Rating:	
			Review of reports of the exposure of data from 100 to 1,000 users, such as names and addresses	Tickets of incidences from JMTSJ web portal.
			Review number of virus alerts	Firewall system logs, IDS logs
			Review number of identified computer/server vulnerabilities	Vulnerability scan reports.

			Low - Incident Rating:	
			Review reports of the exposure of personal data limited to less than 100 users	Tickets of incidences from JMTSJ web portal.
				Firewall system logs
				IDS logs
		Office of CISO are to perform qualitative and quantitative risk assessment of damage reported by the event	Business Impact Analysis (BIA) to be performed for each event, which includes dollar value, number of users affected, security breach findings.	Tickets of incidences from JMTSJ web portal.
				Firewall system logs
				IDS logs
				BIA includes security breach findings if any
				BIA includes results of vulnerability scans if any
				Examples of facts used to assess the severity of reported events
4. Communication	Determine how Information Response team (IRT) will respond and whom to contact about an incident.	Office of CISO are to maintain updated IRT contacts list	Examine whether Computer Services staff know who the members of the IRT are and how to contact them	Current contact list of IRT members.
		CISO will publish the IRT membership		Checklist of contacts by severity rating.
	Ensure that incidents are reported and escalated through the proper channel	**High impact incidents:** Help Desk are to notify the Office of the CISO and the Senior Director. **Medium impact incidents:** The Senior Director is to be notified. **Low impact incidents:** The Help Desk Manager-on-Duty is to be notified.	Review reports of incidents including date, area(s) impacted by incident, severity rating of incident, and escalation process	Tickets of incidences from JMTSJ web portal.
		Incident updates are to be posted periodically on the system status page of the JMTSJNet web Portal.	Review Production Outage Reports	Change Management Application.
5. Incident Management	Ensure CISO create an incident response plan to address specific threats discovered during triage review	Remediation plan timeline and actions are to be created depending on nature of incident.	Review and analyze reports of threat impact findings from the triage stage.	Impact analysis, Threat evaluation, and Quantification reports from triage stage.

	Contain the impact of the incident	Limit exposure of systems, networks, and data	Review records of devices disconnected from network by Incident Response Team (IRT) noting the circumstances under which the incident was detected and reported	Tickets of incidences.
				Intrusion Detection System (IDS) logs.
				Firewall system logs
				Vulnerability scan reports.
	Remove the attacker's access to the environment.	IRT will develop eradication plan of action.	Review and analysis viability of IRT's eradication plan	Eradication plan document.
	Mitigate the vulnerabilities the attacker used to gain and maintain unauthorized access to systems and/or data.	IRT will develop eradication plan of action.	Review and analysis viability of IRT's eradication plan focusing on items that address the vulnerabilities.	Eradication plan document
	Return systems and networks to normal operations	Restore systems from verified backups	Review procedures for the system availability and restoration noting whether or not established procedures were followed.	Documentation of established procedures
				Work logs
				System restores logs
				Documentation of the procedure for backup verification
	Improve policies and procedures to avoid similar incidents in the future	IRT are to develop a comprehensive report on the incident detailing what happened and when.	Review list of policies and procedures updated as a result of IRT findings during postmortem reporting	IRT incident analysis.
				E-mails and/or letters sent to the University community with recommendations for avoiding similar incidents
			Check for similar incidents recorded since the initial incident report	Tickets of incidents.
				Vulnerability scan reports.
6. Roles and Responsibilities	Designate personnel responsible for managing and overseeing incident response	The Office of the CISO is to nominate an Incident Manager for each incident.	Identify number of incidents with a clearly identified Incident Manager	Communications and tickets
				Current list of IRT members and their official titles
		The IRT is to oversee the management of security incidents involving confidential information	Identify number of security incidents involving confidential information which the IRT oversaw	Communications and tickets
		The IRT is to include all appropriate members	Check how IRT members are related to a particular incidence.	Current list of IRT members and their official titles

7. Training	Educate employees and the user community in identifying and mitigating security incidents.	"Lunch and learn" sessions are to be conducted.	Review the number of sessions provided within the past year and the attendance record.	Sessions and attendance list from HR Portal.
				Employee Performance Development Records
				Feedback surveys of attendees
		Training videos are to be posted on the organization intranet.	Review number of hits on the video to see popularity	Training videos on the JMTSJ web portal