Safe Systems

Incident Handling Checklist

(Based on NIST[1], modified for financial institutions[2])

Description of incident:			
Action		**Date / Time Completed**	**Initials**
Detection and Analysis			
1.	CSIRT (or equivalent) should determine whether an incident has occurred, and whether it should be classified as an intrusion.		
1.1	Analyze the precursors and indicators		
1.2	Look for correlating information		
1.3	Perform research (e.g., search engines, knowledge base)		
1.4	As soon as the CSIRT believes an incident has occurred, begin documenting the investigation and gathering evidence		
2.	Prioritize handling the incident based on the relevant factors and the level of severity (functional impact, information impact, recoverability effort, etc.)		
3.	Report the incident to the appropriate internal and external parties and organizations (regulators, customers, and/or law enforcement)		
Containment, Eradication, and Recovery			
4.	Acquire, preserve, secure, and document evidence		
5.	Contain the incident		
6.	Eradicate the incident		
6.1	Identify and mitigate all vulnerabilities that were exploited		
6.2	Remove malware, inappropriate materials, and other components		
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them		
7.	Recover from the incident		
7.1	Return affected systems to an operationally ready state		
7.2	Confirm that the affected systems are functioning normally and meet existing base-line configuration standards		
7.3	If necessary, implement additional monitoring to look for future related activity		
Post-Incident Activity			
8.	Create a follow-up report		
9.	Hold a lessons learned meeting to identify control failures and whether control changes/additions are necessary		
10.	If necessary, prepare and file a Suspicious Activities Report (SAR)		

[1] Full NIST guide is here: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf, original table on page 42.
[2] FFIEC guidance is here: http://ithandbook.ffiec.gov/it-booklets/information-security/security-monitoring/analysis-and-response/intrusion-response.aspx.