Grey County Policy Manual	"x" Incident Response Dept: Corporate Services, IT Division Committee: TBD

PURPOSE

The Incident management workflow / process ensures that an orderly sequence is followed when an incident is declared. Additionally, it ensures that the right resources are involved in identifying and declaring an incident.

SCOPE

IN SCOPE

The process described in this document applies to the following:

1. All COUNTY OF GREY internal departments
2. All business partners handling or storing COUNTY OF GREY sensitive information, or sensitive information of a 3rd party for which COUNTY OF GREY is responsible.

All departments or partners must agree to the disclosure of any event relating to the security of our infrastructure or the facilities and systems processing or containing sensitive information (including peripheral systems such as infrastructure services) as per this process.

For definition purposes, a suspected data breach is any suspicion that information systems containing COUNTY OF GREY information has been compromised. The term sensitive information refers to ANY COUNTY OF GREY data asset.

OUT OF SCOPE

Incidents of an operational nature, involving infrastructure, or in any way not directly affecting the security of sensitive information are not in scope and should be referred to the relevant departments (IT, DEV, etc.) via the helpdesk.

KEY ROLES AND RESPONSIBILITIES

The following are the roles and responsibilities of the employees of COUNTY OF GREY and its partners with regards to security incidents:

- **All employees (Both COUNTY OF GREY, contractors and partners)**
  - Declare any security event to the 1st line support organization (Helpdesk: **support email** or **support #**). Alternatively, it is possible to contact The

Information Security (InfoSec) Lead directly, but this should be avoided. Going through the helpdesk is encouraged. Certain departments, such as IT or Helpdesk staff will report events directly to the Information Security Lead. The Information Security Lead can be reached at #.

- **Helpdesk (COUNTY OF GREY or partners 1st line internal support apparatus)**
  - Receive, complete and record incident declarations.
  - Perform a quick preliminary analysis to determine whether incident is security related. Escalate until determination can be made. Forward Security Incidents to Information Security (InfoSec) Lead.

- **IT**
  - Promptly authorize expenditures for incident containment, response and investigation services.

- **Information Security – Information Security Lead / Information Security team**
  - Confirm, accept, and document Information Security (InfoSec) incidents.
  - Coordinate incident response, including containment.
  - Collect or manage the collection of any evidence.
  - Report Incident to management based on the documented severity and escalation flow chart
  - Declare the incident closed (contained)
  - Provide guidance in remediation and operational improvements.
  - Follow up on agreed upon remediation and operational improvements
  - Declare the event closed once agreed upon remediation and improvements are in place

- **Business Partners**
  - Properly declare relevant incidents per this process and its definitions.
  - Provide a point of contact for incident reporting and response.
  - Provide expertise and support as needed for incident handling and response.

- **HR, Legal, Procurement, Communications**
  - Provide expertise and support in dealing with human resources, potential legal liabilities, Contractual issues, and issues relating to the organization's public image.

DEFINITIONS

The definition of an Information security incident is any incident where:
*There is knowledge **or suspicion** that the confidentiality, availability or integrity of COUNTY OF GREY Information Assets have been compromised.*

In this document a *Security* or *Information Security* Incident refers to a *directed* attack intended to compromise the confidentiality, integrity, or availability of data as defined above. This is commonly referred to as a *data breach* or *security breach*. These events should not be confused with *operational security* events or incidents that take place commonly and are addressed by other processes and internal operational teams.

Some incidents such as Spam, Virus & Malware are known as *operational* security incidents and are handled via regular operational incident management (Helpdesk).
These operational incidents are accounted for in the process but are redirected to the appropriate entity's (site/project/partner) regular operational incident management process.

A ransomeware outbreak for example can have a major impact on the enterprise but is still considered an operational event unless the investigation performed by the IT operations department determines that the malicious code (virus) was collecting sensitive information therefor resulting in a data breach event. Information Security is only brought into the loop when a possible compromise of information (data breach) is suspected.

> EXAMPLE 1: A users workstation appears to be infected by a virus.
>
> In this example, the helpdesk can process this event as an operation event. During the course of the resolution of this event, if it is found that the virus in question allowed the control of the workstation remotely, or captured sensitive information, then this would become an incident to be managed using this incident management process and the event would be re-categorized and treated as such.
>
> EXAMPLE 2: A network administrator observes unidentified network activity between the corporate network and Internet addresses in a foreign country not serviced by the enterprise. This should be processed through this incident management process.
>
> **IMPORTANT NOTE:** When in doubt, use this process and advise the InfoSec team.

Note that disasters such as fire or flood are handled through the business continuity (BCP) and the disaster recovery (DR) plans and fall outside of the scope of this document.

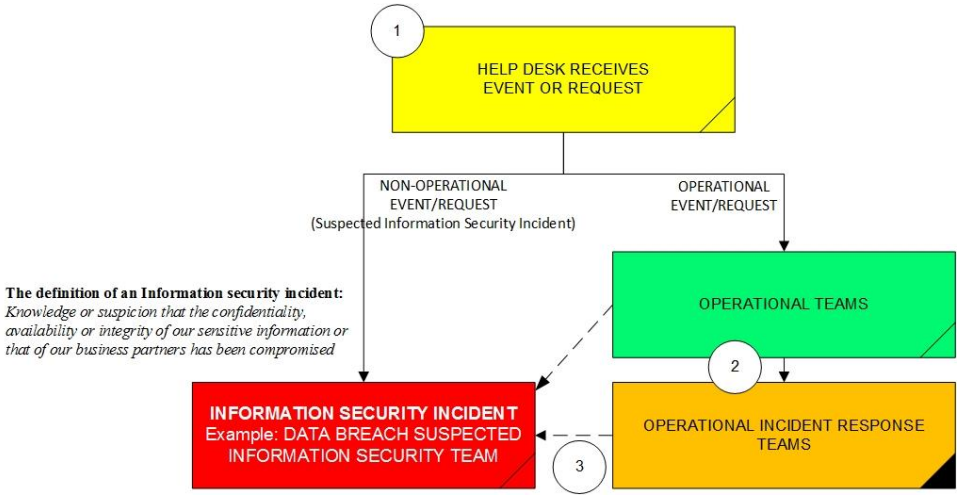
Information Security Team
Security incidents can happen at any time of day. For this reason, we refer to the Information Security Role as a "Team". Ideally, more than one person should comprise this function. In this document, the term "Information Security", "Information Security Team" and "Information Security Lead" all refer to the same function.

One of the Information Security team's primary duties is to protect COUNTY OF GREY's Intellectual Property and sensitive data assets. This process defines only incidents that are the responsibility of the information Security team and therefore the definition of an *Information Security* Incident is an important one. There are many types of security incidents, and this process does not apply to all of them.

PROCESS

The high-level process can be summed up as follows:

1) The helpdesk receives an event or request. They determine if it is a normal operational event that should be handled by the various operational teams or if it is a potential data breach related event that should be sent to Information Security.
2) For serious (high impact) operational events, the various operational teams can contact their respective Incident Response Team for assistance.
3) The Incident Response team could conclude that a data breach may have taken place and notify Information Security



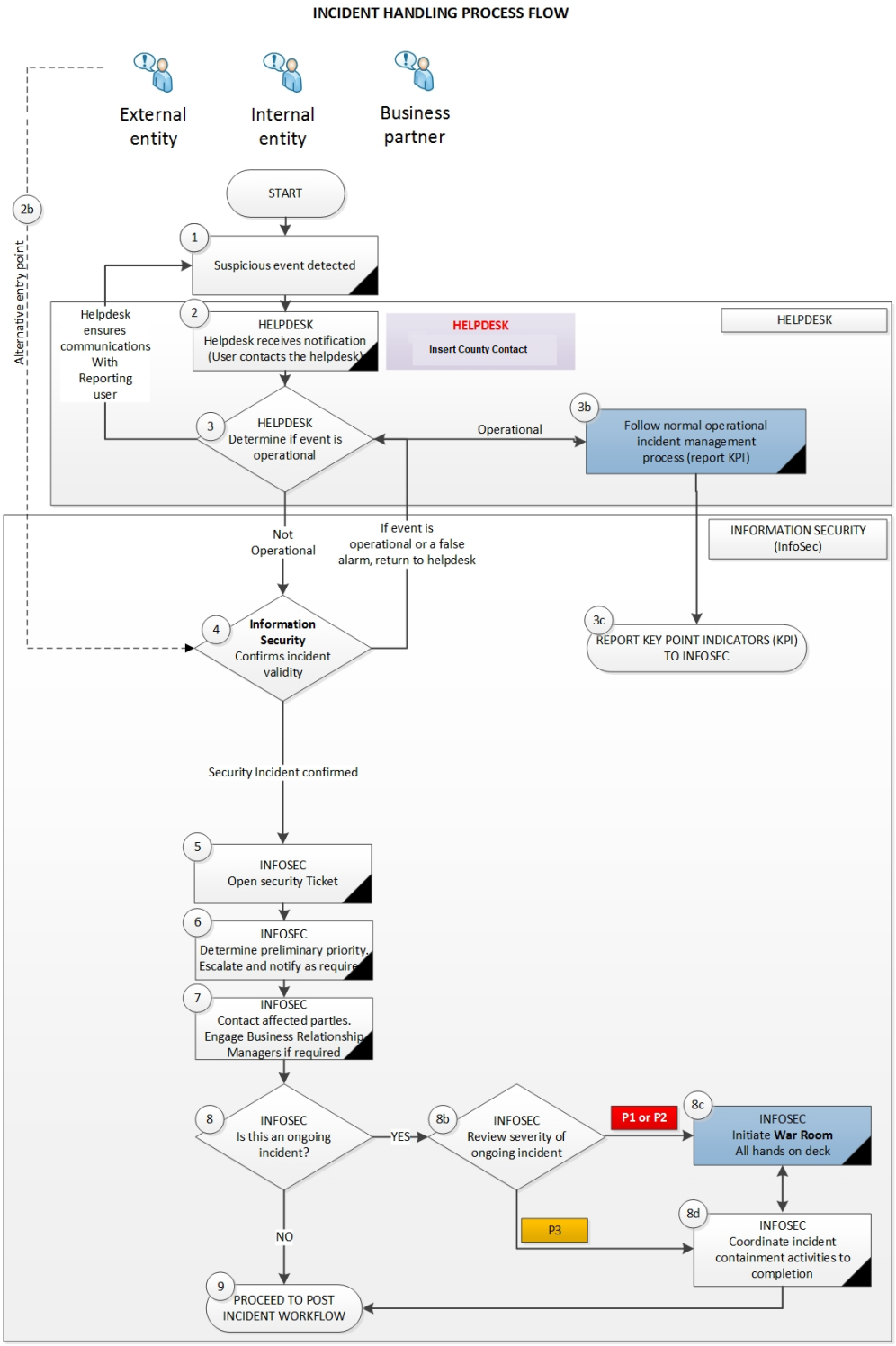
PROCESS DESIGN

There are 2 main parts to the COUNTY OF GREY Information Security Incident Response process:

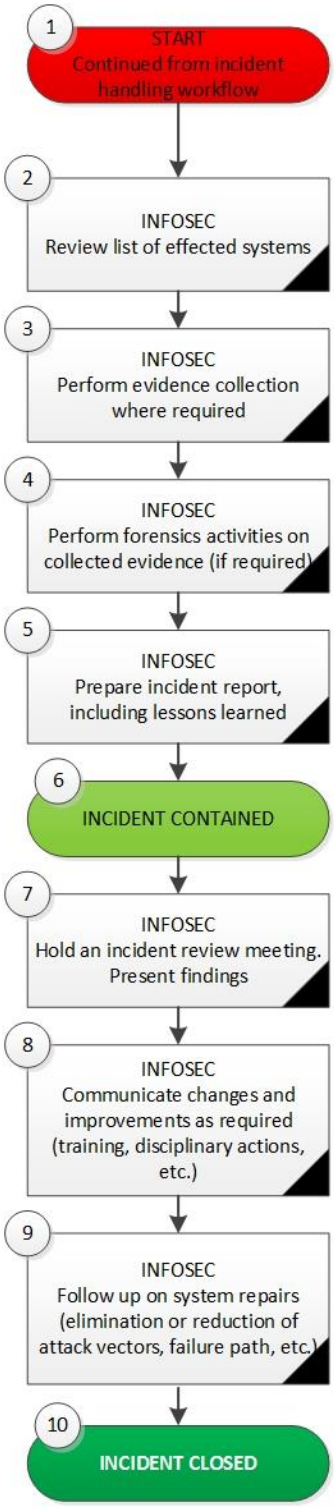
- PART 1: Incident handling
  - The helpdesk is the focal point for notifying incidents or suspicious events or behavior. The helpdesk determines if information security's involvement is required or if the events are of an operational nature and should be handled as such. The first steps are generic steps that can be used with any support/helpdesk framework irrespective of site, project, or company (in the case of partners).

- PART 2: Post incident handling
  - Once an incident is under control (resolved/contained) a post incident review is required. An incident can have one of three statuses; TICKET OPEN, INCIDENT CLOSED, and TICKET CLOSED. Only once the incident has been understood with a post mortem can the event ticket be closed. A post mortem document must be produced.

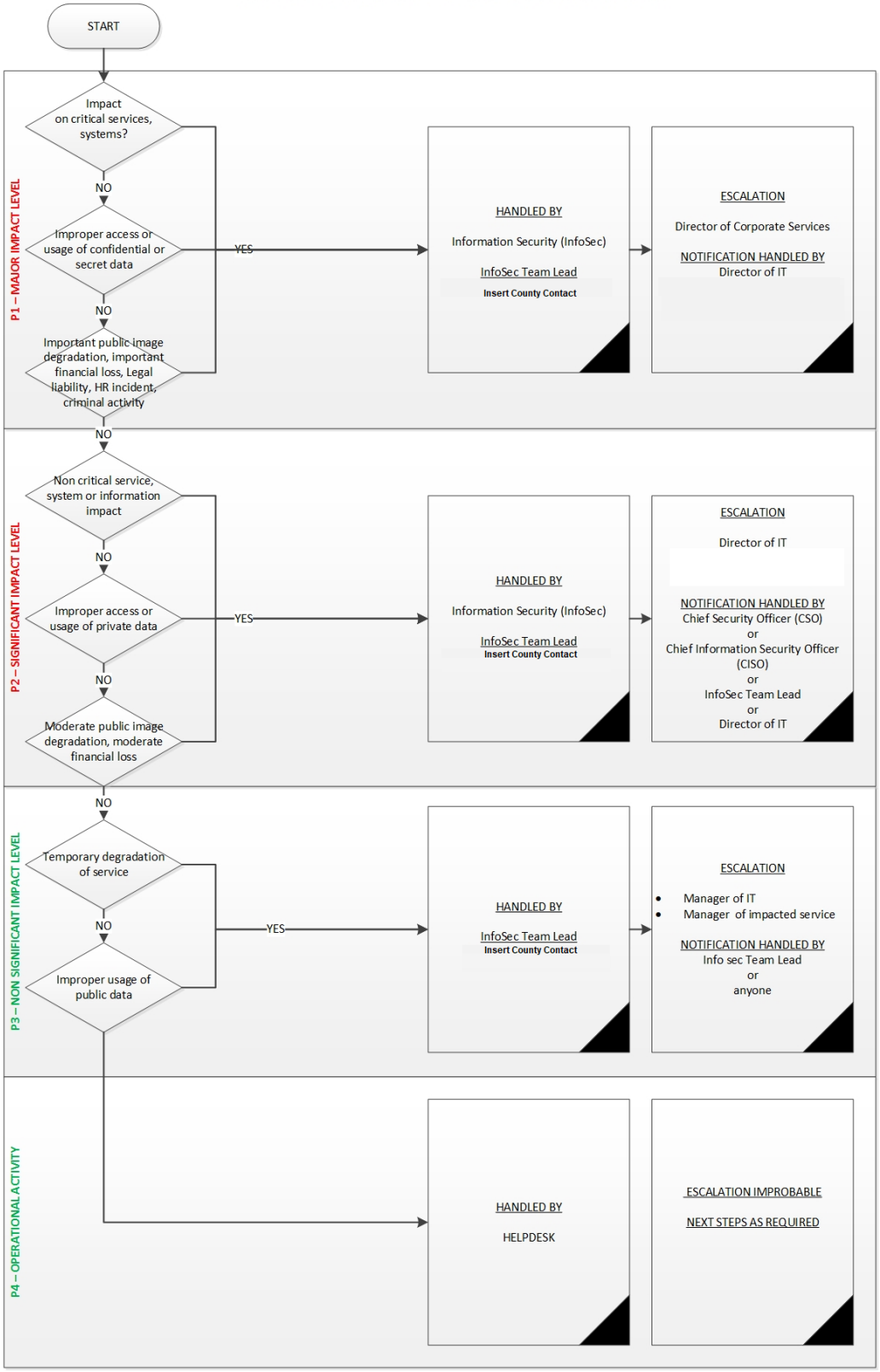
PROCESS WORKFLOW



POST-INCIDENT HANDLING PROCESS FLOW



SEVERITY LEVEL AND ESCALATION FLOWCHART



PROCESS DESCRIPTION

This section describes each step of the process as per each reference/step number in the workflow diagram.

INCIDENT HANDLING PROCESS WORKFLOW

1. A user suspects an incident. At this point it may not be clear whether or not this is a security incident.

2. The user contacts their respective Helpdesk and provides the details of the suspected incident.

2b. Alternatively, it is possible to contact information security directly, but this should be avoided. Going through the helpdesk is encouraged. Certain departments, such as monitoring will report events directly to Information Security

3. The Helpdesk must determine if the incident is operational or Information Security related.

3b. if this issue is of an operational nature, the helpdesk follows the normal incident management process.

- If this is considered an incident, the local Incident Response Team should be tasked with the event.
- If at some point, the Incident Response Team believes that a data breach may have taken place, Information Security is notified

3c. Key point indicators are reported back to Information Security.

4. If the incident is not operational but indeed a security event, COUNTY OF GREY Information Security is notified of the incident and confirms whether the incident is Information Security related. If so, COUNTY OF GREY Information Security accepts the incident and assigns an incident coordinator. If not, the incident is sent back to the support organization that submitted it along with the explanation that justifies the return.

5. The COUNTY OF GREY Information Security Incident Coordinator opens a Security ticket in the incident database.

6. COUNTY OF GREY Information Security performs an initial analysis of the situation to determine the incident's classification (P4 to P1). The incident coordinator then escalates as appropriate for the given incident classification. (See Classification and Escalation & Notification - Sections 9 & 10 respectively). Note that the classification must continuously be adjusted as new information becomes available.

The HR, Legal, Communications, and Procurement (Supply Chain) departments should also be involved at this stage if they are needed based on the type of incident.

7. Contact departments affected by the incident.
(see section 8.1).

8. COUNTY OF GREY InfoSec determines if the incident or vulnerability leading to the incident is ongoing. If yes, proceed to Step 8b.

If YES (ongoing incident=Yes)
8b. Validate incident classification.
If P1 or P2 proceed to step 8c (Initiate War room protocol)
If incident is a P3 proceed to step 8d (coordinate containment/resolution)
If incident is a P4 (false positive) return to helpdesk for resolution

8c. Initiate War Room protocol. As this is a high priority incident, the War Room protocol (all hands on deck) should now be invoked to maximize response. Continue to step 8d as needed.

8d. Coordinate incident containment activities to completion. Information Security provides leadership to support departments in performing containment activities (as detailed in section 6.1). Existing state of any data, system or configuration could be evidence and should therefore be recorded prior to any changes. Proceed to step 9 when completed.

9. Proceed to POST INCIDENT WORKFLOW

POST-INCIDENT HANDLING WORKFLOW

1. This process starts following the completed management of an incident from the INCIDENT HANDLING PROCESS FLOW.

2. Information Security (InfoSec) reviews the list (gathers the information) of all effected systems.

3. Information Security provides guidance and instructions to support departments to collect and assemble relevant evidence.

4. InfoSec assists in collecting evidence (if required) and performing forensics analysis.

5. The Information Security incident coordinator completes the Information Security Incident Report form and notes any lessons learned, investigation conclusions, etc.

6. This marks the end of the active phase of the incident. As an example, the breach has been contained (and understood) and no more information is being lost, systems that were under attack are once again available, safe, etc. All relevant evidence has been collected from affected systems.

7. Coordinate an incident review meeting to present the findings. Provide completed incident report to CISO for dissemination as appropriate. Lessons learned should be reviewed and converted into actionable steps to prevent or mitigate similar events in the future. If an internal resource was deemed at fault or negligent without further investigation being needed, disciplinary action should be taken at this stage.

8. The actions identified to prevent or mitigate recurrence of the incident should be submitted to stakeholders and implemented. In the case of any ongoing investigations against internal resources or third parties, these should be completed and reported to the relevant management.

9. Follow up on system repairs or any other modifications that need to be done, until all targeted changes are completed (or minimally acknowledged). This is required in order to eliminate or reduce attack vectors or failure paths to minimize event reoccurrence.

NOTE: Any lessons learned affecting the general user population should be disseminated via on boarding and other outlets (company portal, posters, announcements, etc). In the case of a partner being at fault, contractual addendums should be negotiated to ensure they implement the proper controls. If any investigations were completed, relevant disciplinary or legal action should be taken at this stage. This marks the end of the Security Incident Process.

10. Event complete. Incident closed. At this point, all relevant actions have been taken and the event can now be considered closed. The ticket can be closed in the InfoSec system.

References

None.

Related Documents

None.

Approval and Ownership

Created By	Title	Date	Signature
Gary J. Walker			
Approved By	**Title**	**Date**	**Signature**

Revision History

Version	Revision Date	By	Description

RACI DIAGRAM (SAMPLE FOR GREY)

Description of task / Business component	COUNTY OF GREY Staff Consultants Resource Third party	Helpdesk	Local Incident Response Team	Information Technology (IT)	Information Security (InfoSec) Team Lead	Chief Information Security Officer (CSO/CISO)	Director of Impacted services	Manager / Director of IT	Director of corporate services	HR	LEGAL	Communications
Report possible security violation	R	I			A							
Determine if event is operational or not (data breach oriented)	C	R			A	I						
Handle operational incidents			R	A		I				C	C	C
Confirm if an incident is of Information Security nature)				I	R	A						
Categorize incident level					R	A	I					
Escalation for Level 3 events (Medium severity)				I	C	R	A			C	C	C
Escalation for Level 2 events (High severity)				I	C	R		A		C	C	C
Escalation for Level 1 events (Critical severity)				I	C	C		R	A	C	C	C
Coordinate incident response, including containment		I	C	C	R	A	C					
Collect and manage evidence				C	R	A				I	I	
Review Human Resources impact						I				R	C	C
Review Legal impacts			I	I	I	I	I			C	R	C
Prepare official communications		I	I	I	I	I	I	A	I	C	C	R
Declare incident contained		I	I	I	R	A	I	I	I			
Conduct post incident review		I	C	C	R	A	C	I	I	C	C	
Follow up on long term remediation requirements		I	C	C	R	A	C	I	I	I	I	
Declare the incident closed		I	I	I	R	A	I	I	I			

- **Responsible:** person who performs an activity or does the work.
- **Accountable:** person who is ultimately accountable and has Yes/No/Veto.
- **Consulted:** person that needs to feedback and contribute to the activity.
- **Informed:** person that needs to know of the decision or action.