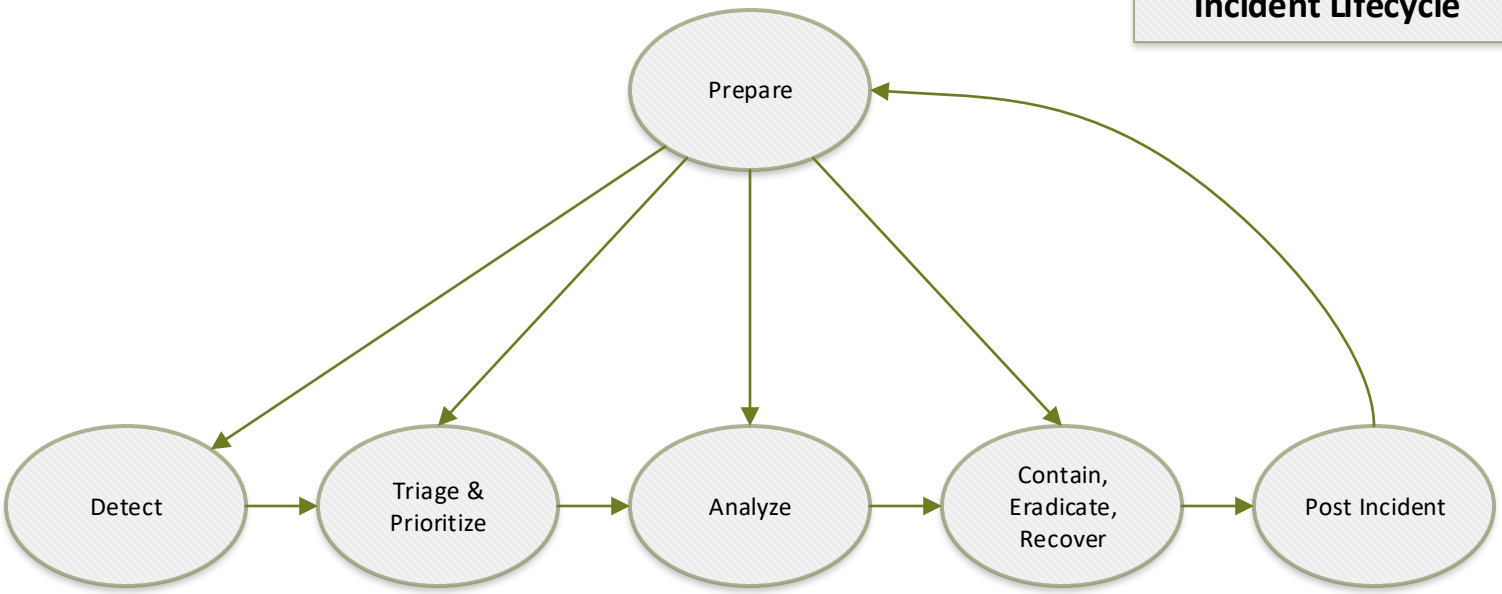
Incident Lifecycle



This work is licensed under Creative Commons Attribution-ShareAlike 4.0

https://creativecommons.org/licenses/by-sa/4.0/

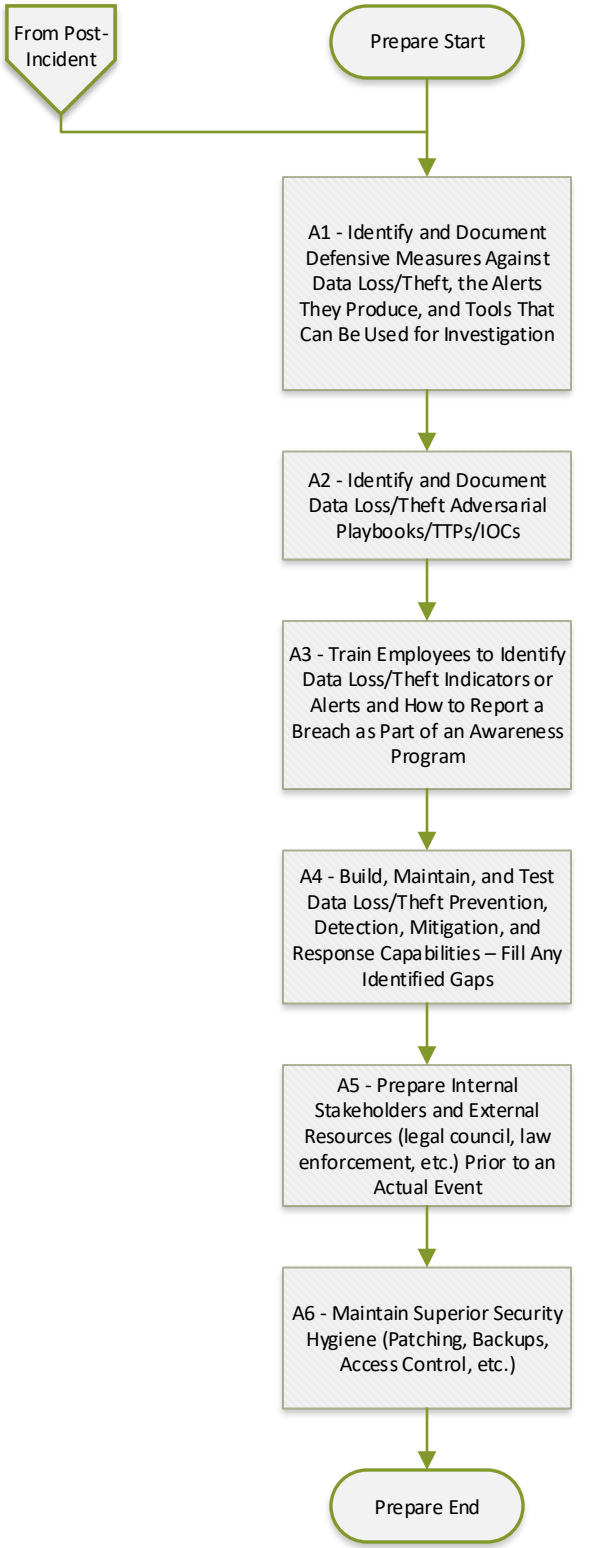
Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

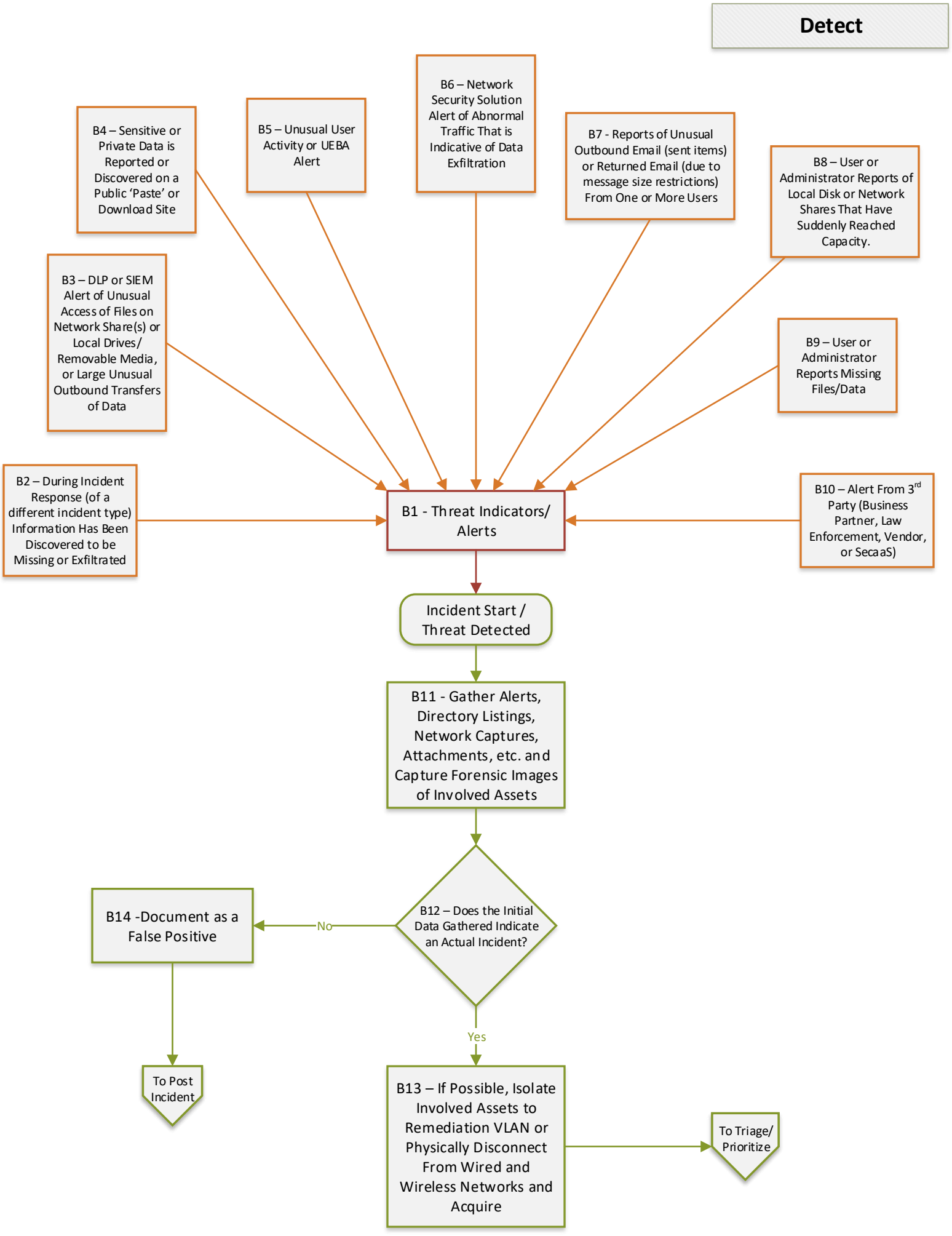
ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

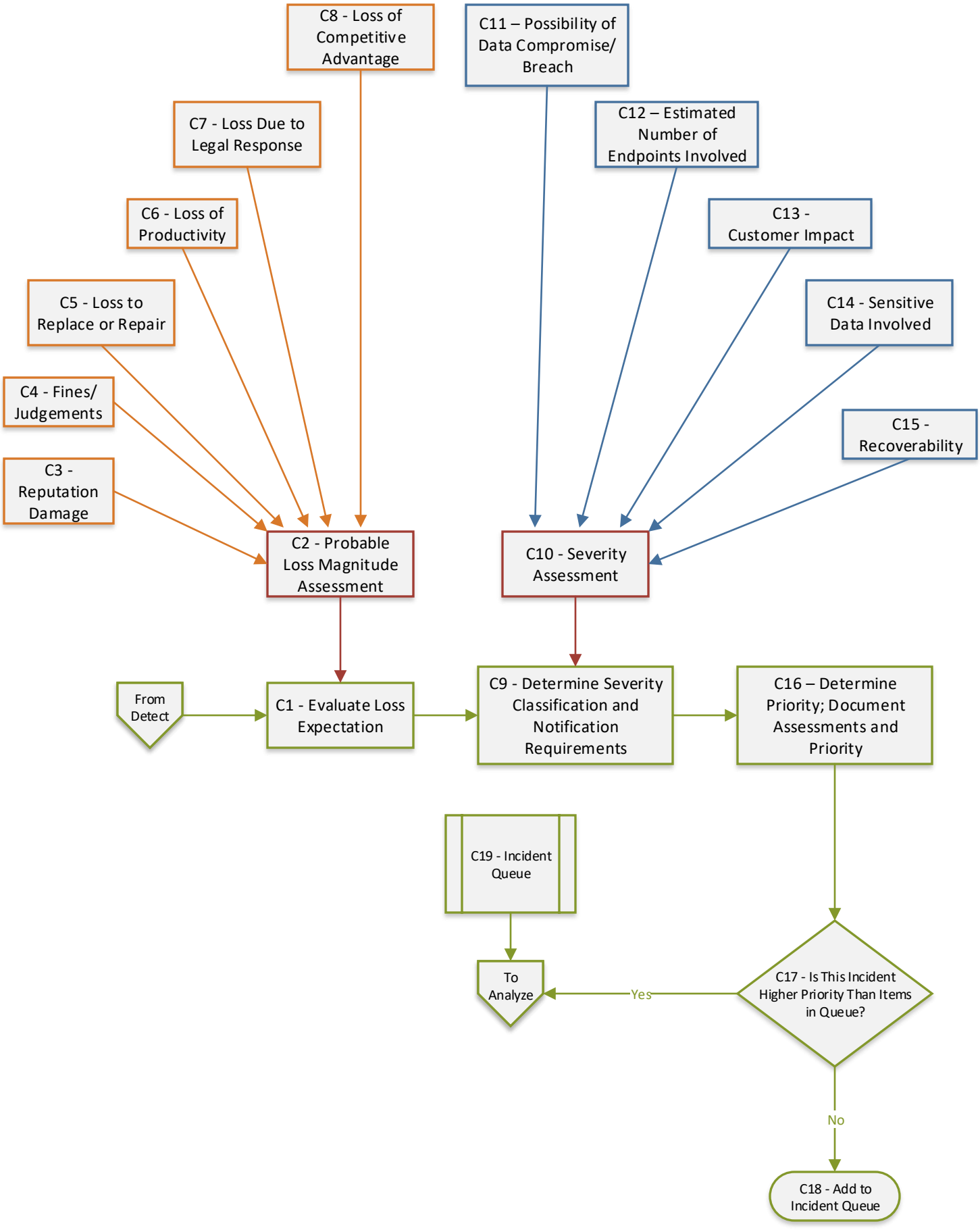
Copyright 2016, 2019 Joshua C Geno

Prepare

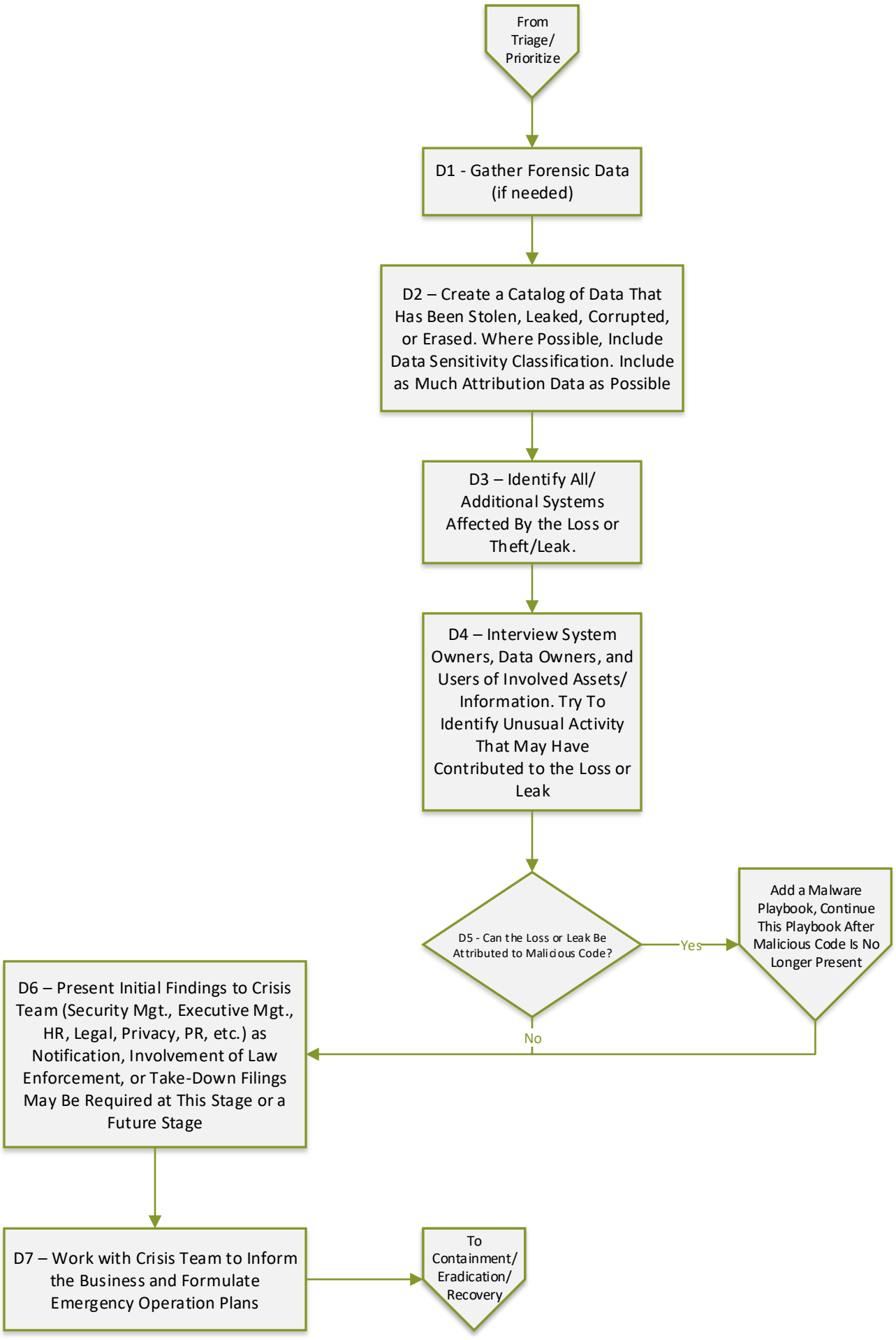

From Post-Incident
Prepare Start
A1 - Identify and Document Defensive Measures Against Data Loss/Theft, the Alerts They Produce, and Tools That Can Be Used for Investigation
A2 - Identify and Document Data Loss/Theft Adversarial Playbooks/TTPs/IOCs
A3 - Train Employees to Identify Data Loss/Theft Indicators or Alerts and How to Report a Breach as Part of an Awareness Program
A4 - Build, Maintain, and Test Data Loss/Theft Prevention, Detection, Mitigation, and Response Capabilities – Fill Any Identified Gaps
A5 - Prepare Internal Stakeholders and External Resources (legal council, law enforcement, etc.) Prior to an Actual Event
A6 - Maintain Superior Security Hygiene (Patching, Backups, Access Control, etc.)
Prepare End


Detect
B4 – Sensitive or Private Data is Reported or Discovered on a Public 'Paste' or Download Site
B5 – Unusual User Activity or UEBA Alert
B6 – Network Security Solution Alert of Abnormal Traffic That is Indicative of Data Exfiltration
B7 - Reports of Unusual Outbound Email (sent items) or Returned Email (due to message size restrictions) From One or More Users
B8 – User or Administrator Reports of Local Disk or Network Shares That Have Suddenly Reached Capacity.
B3 – DLP or SIEM Alert of Unusual Access of Files on Network Share(s) or Local Drives/ Removable Media, or Large Unusual Outbound Transfers of Data
B9 – User or Administrator Reports Missing Files/Data
B2 – During Incident Response (of a different incident type) Information Has Been Discovered to be Missing or Exfiltrated
B1 - Threat Indicators/ Alerts
B10 – Alert From 3rd Party (Business Partner, Law Enforcement, Vendor, or SecaaS)
Incident Start / Threat Detected
B11 - Gather Alerts, Directory Listings, Network Captures, Attachments, etc. and Capture Forensic Images of Involved Assets
B12 – Does the Initial Data Gathered Indicate an Actual Incident?
No
B14 -Document as a False Positive
To Post Incident
Yes
B13 – If Possible, Isolate Involved Assets to Remediation VLAN or Physically Disconnect From Wired and Wireless Networks and Acquire
To Triage/ Prioritize

Triage/Prioritize



Analyze


From Triage/ Prioritize
D1 - Gather Forensic Data (if needed)
D2 – Create a Catalog of Data That Has Been Stolen, Leaked, Corrupted, or Erased. Where Possible, Include Data Sensitivity Classification. Include as Much Attribution Data as Possible
D3 – Identify All/ Additional Systems Affected By the Loss or Theft/Leak.
D4 – Interview System Owners, Data Owners, and Users of Involved Assets/ Information. Try To Identify Unusual Activity That May Have Contributed to the Loss or Leak
D5 - Can the Loss or Leak Be Attributed to Malicious Code?
Yes
Add a Malware Playbook, Continue This Playbook After Malicious Code Is No Longer Present
No
D6 – Present Initial Findings to Crisis Team (Security Mgt., Executive Mgt., HR, Legal, Privacy, PR, etc.) as Notification, Involvement of Law Enforcement, or Take-Down Filings May Be Required at This Stage or a Future Stage
D7 – Work with Crisis Team to Inform the Business and Formulate Emergency Operation Plans
To Containment/ Eradication/ Recovery

Contain/Eradicate/ Recover

From Analyze

E1 -Data Loss (Erasure/Corruption) or Theft/Leak?

Loss

E2 – If New Evidence was Obtained in D6, Chain the Loss (Investigative Chains) Backward and Forward Until You Discover the Source of the Loss and All Involved Assets, Data, and Credentials

E3 –Remediate Loss/Corruption Source.

E4 – Was a System Compromised or Breached?

Yes

Add System Compromise/Breach Playbook, Continue This Playbook

No

E5 - Were Local or Network Credentials Involved?

Yes

Add Authority/ Credential Misuse Playbook, Continue This Playbook

No

E6 - Was a Malicious Insider Involved?

Yes

E7 – Double Check and Sanity Check the Evidence. Accusations of Insider Data Loss/Corruption Will End a Career

Add Suspicious User Activity (Insider Threat) Playbook, Continue This Playbook

No

E8 – Inform the Crisis Team. Provide All Relevant Evidence to HR and Legal. At HR/Legal's Direction, Suspend Insider's Credentials and (Where Possible) Physical Access, Seize Corporate Assets

E9 - Backups Available of Deleted or Corrupted Files or Systems?

No

E10 – Work with Crisis Team to Inform System Owners, Data Owners, and Users

E11 – Implement Previously Identified (in D7) Alternative Courses of Action and Work-Arounds

Yes

E12 - Restore Deleted Files or Systems

E13 – Inform System and Data Owners. Perform System Testing

E14 – Inform Crisis Team, Business and Users. Perform User Acceptance Testing

E31 – Work With System and Data Owners To Complete Recovery Activities. Perform System Testing

Theft/Leak

E16 – If New Evidence was Obtained in D6, Chain the Theft/ Leak (Investigative Chains) Backward and Forward Until You Discover the Internal or External Breach Source and All Involved Assets, Data, and Credentials

E17 – Work With Available Legal Resources and, If Needed, Law Enforcement to Investigate the Theft/Leak With Involved Web Services and Providers

E18 – Where Data Resides on an Unauthorized Third Party (Download or 'Paste' Site), Work With Available Legal Resources to File Take-Down Requests With Involved Web Services and Providers (If This Hasn't Already Been Completed)

E19 –Capture Forensic Data from Newly Identified Involved Assets (If Needed)

E20 –Analyze Collected Data and Interviews to Determine Source of Theft/Leak.

E21 -Can The Theft or Leak Be Attributed to Unintentional Misconfiguration?

Yes

E22 – Engage Internal and Vendor Support Resources to Correct the Misconfiguration and Restore Positive Control

E23 – Perform System Testing to Ensure Functionality Has Not Been Affected

E24 – Inform Crisis Team, Business and Users. Perform User Acceptance Testing

No

E25 – Was a System Compromised or Breached?

Yes

Add System Compromise/Breach Playbook, Continue This Playbook

No

E26 - Were Local or Network Credentials Involved?

Yes

Add Authority/ Credential Misuse Playbook, Continue This Playbook

No

E27 - Was a Malicious Insider Involved?

Yes

E28 – Double Check and Sanity Check the Evidence. Accusations of Insider Data Theft/Leak Will End a Career

Add Suspicious User Activity (Insider Threat) Playbook, Continue This Playbook

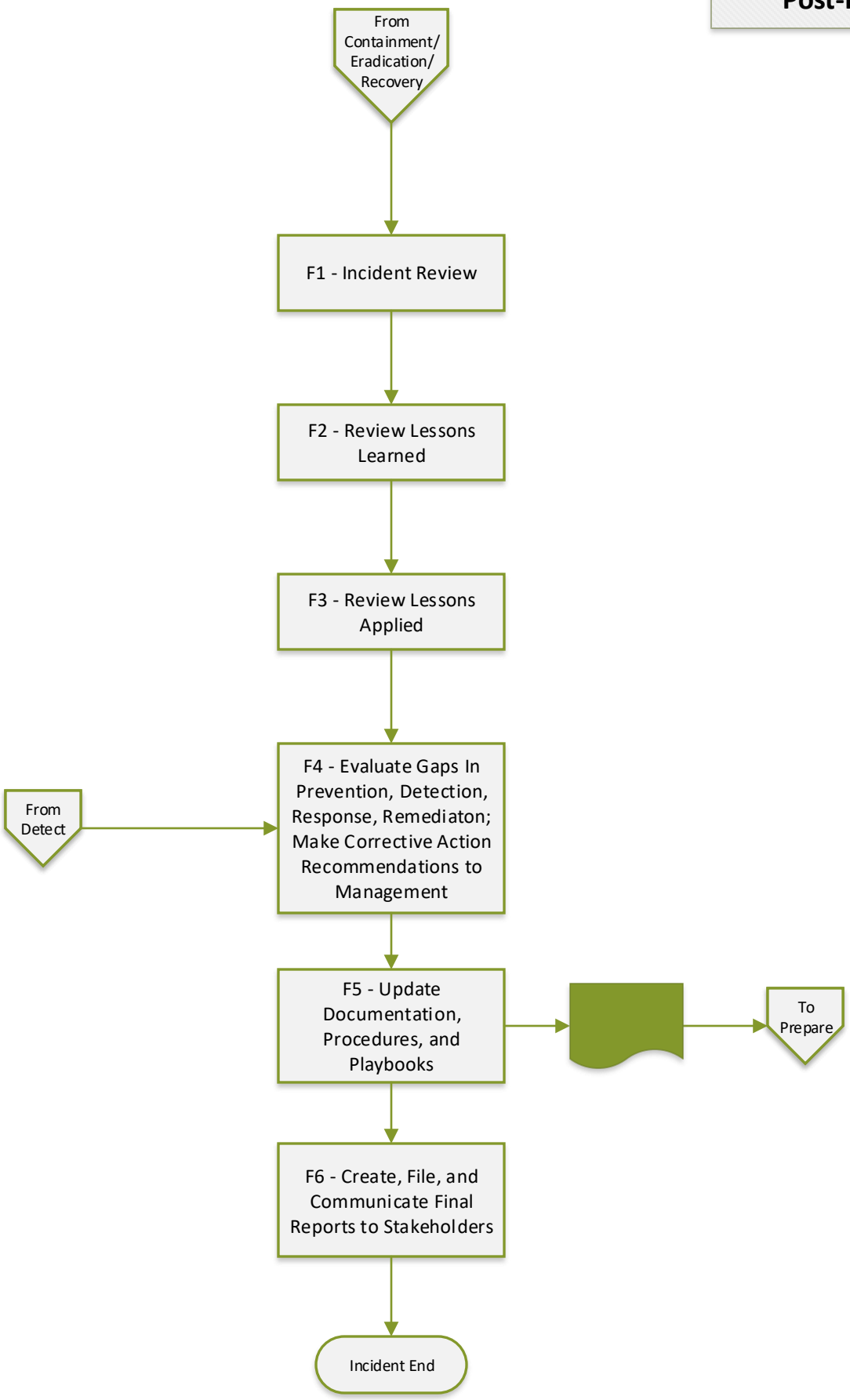
E29 – Inform the Crisis Team. Provide All Relevant Evidence to HR and Legal. At HR/Legal's Direction, Suspend Insider's Credentials and (Where Possible) Physical Access, Seize Corporate Assets

No

E30 – Are There Outstanding Recovery Activities?

Yes

E15 - Apply Patches, Security Products, Additional Controls, Enhance Awareness Training, Enhanced Procedures or Other Mitigations to Prevent Loss or Theft/Leak via Similar Scenario

To Post-Incident

Post-Incident