

M I C R O S O F T I N C I D E N T R E S P O N S E

Navigating the Maze of Incident Response

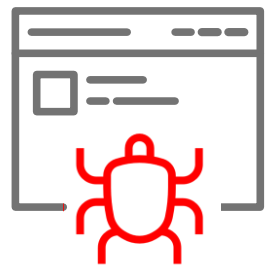


Introduction

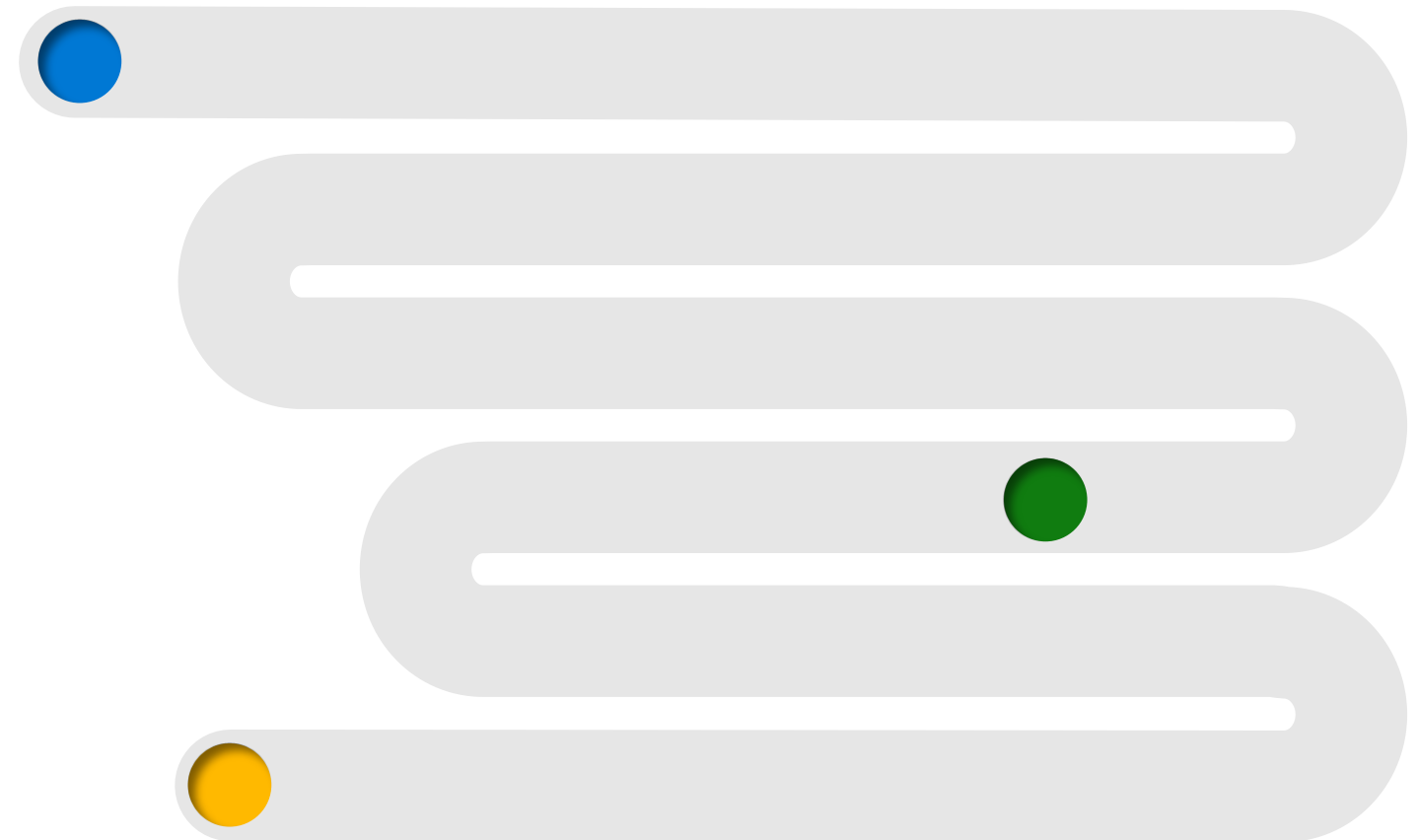
Cyber security incidents are an inevitability. It's important to start an incident response (IR) the right way, with a thorough understanding of what to do, when to do it, and who needs to be involved. Beyond the obvious questions about the scope of the compromise and how to regain control, it's important to preserve evidence, as well as understand your compliance and regulatory obligations.

This guide explains how to structure an incident response, with recommendations and best practices to help navigate those crucial initial hours after a breach is detected.

While a wealth of material on IR best practices already exists, **this document focuses first and foremost on the people and processes involved in effectively responding to an incident**—the roles required to respond to incidents, how to manage your response in way that is efficient and people-centric, how to avoid burnout and ensure all requirements and obligations are met at every level, and how to ensure everyone's roles and responsibilities are clear, so the incident response is effective overall.



Cyber security incidents are an inevitability. It's important to start an incident response (IR) the right way.



Navigating the Maze

As enterprise networks grow in both size and complexity, securing them from motivated threat actors becomes even more challenging. The incident response process becomes a maze which security professionals must learn to navigate.

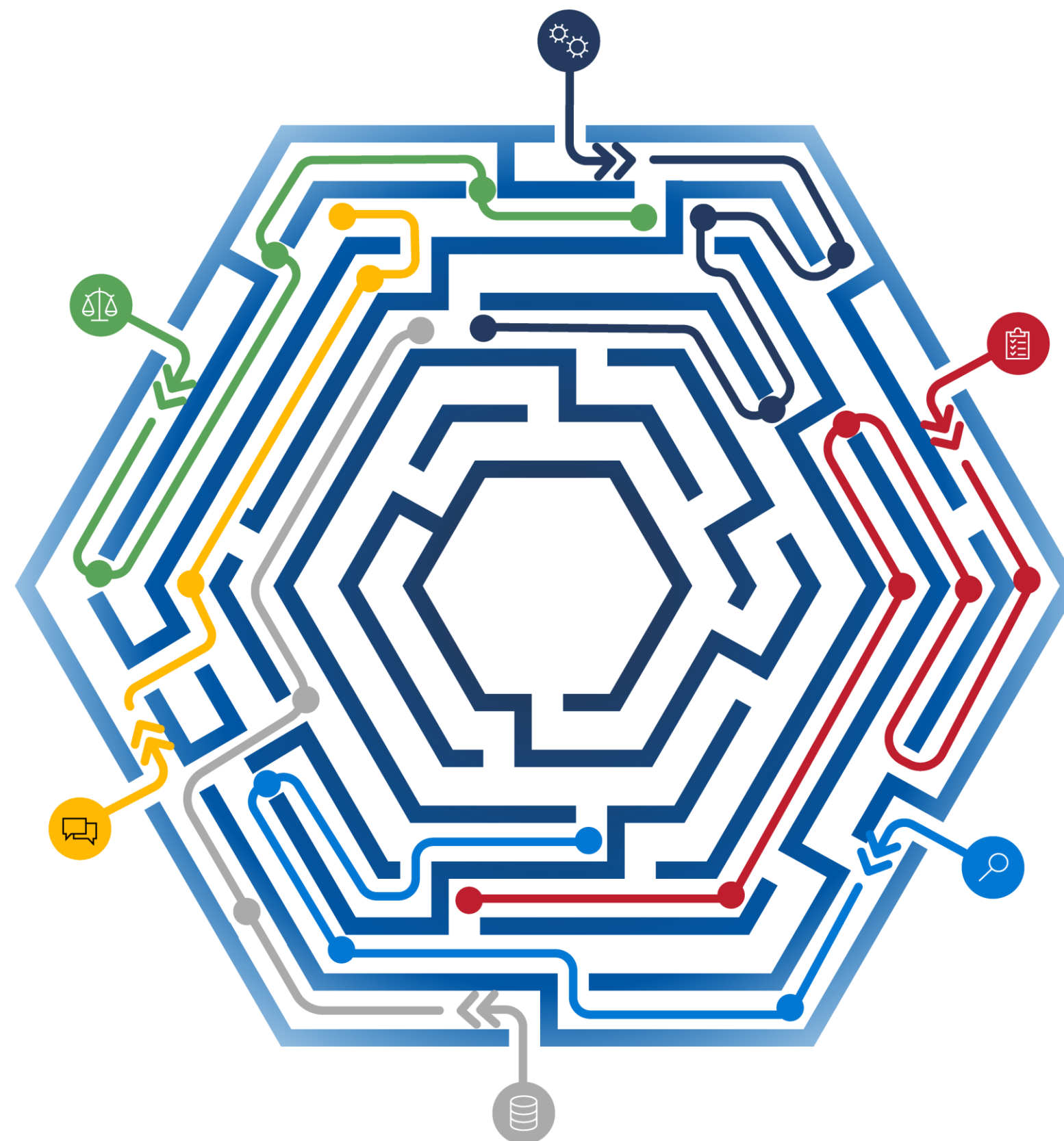
A study on cyber resiliency conducted by IBM determined that **only 26% of organizations have an incident response plan which is consistently applied**. Yet having a well-thought-out incident response plan—a map for the maze—can be the point of difference between quickly containing a threat actor and having to spend a significant amount of time (and money) rebuilding assets or addressing wide-spread business impact.

Some organizations do have battle-tested incident response plans and business processes in place to quickly address an intrusion, often based on best practice guidance. But knowing more about how to navigate the maze of incident response can make a significant impact on your organization's recovery time and cost.

This guidance was developed by the Microsoft Incident Response team from their time in the field supporting customers. It is designed to address some of the common issues and pitfalls encountered during the outset of a response.

Take note: this guidance is not intended to replace comprehensive incident response planning, which should occur outside of a live incident, but as tactical guidance to help both security teams and senior stakeholders navigate an incident response investigation.

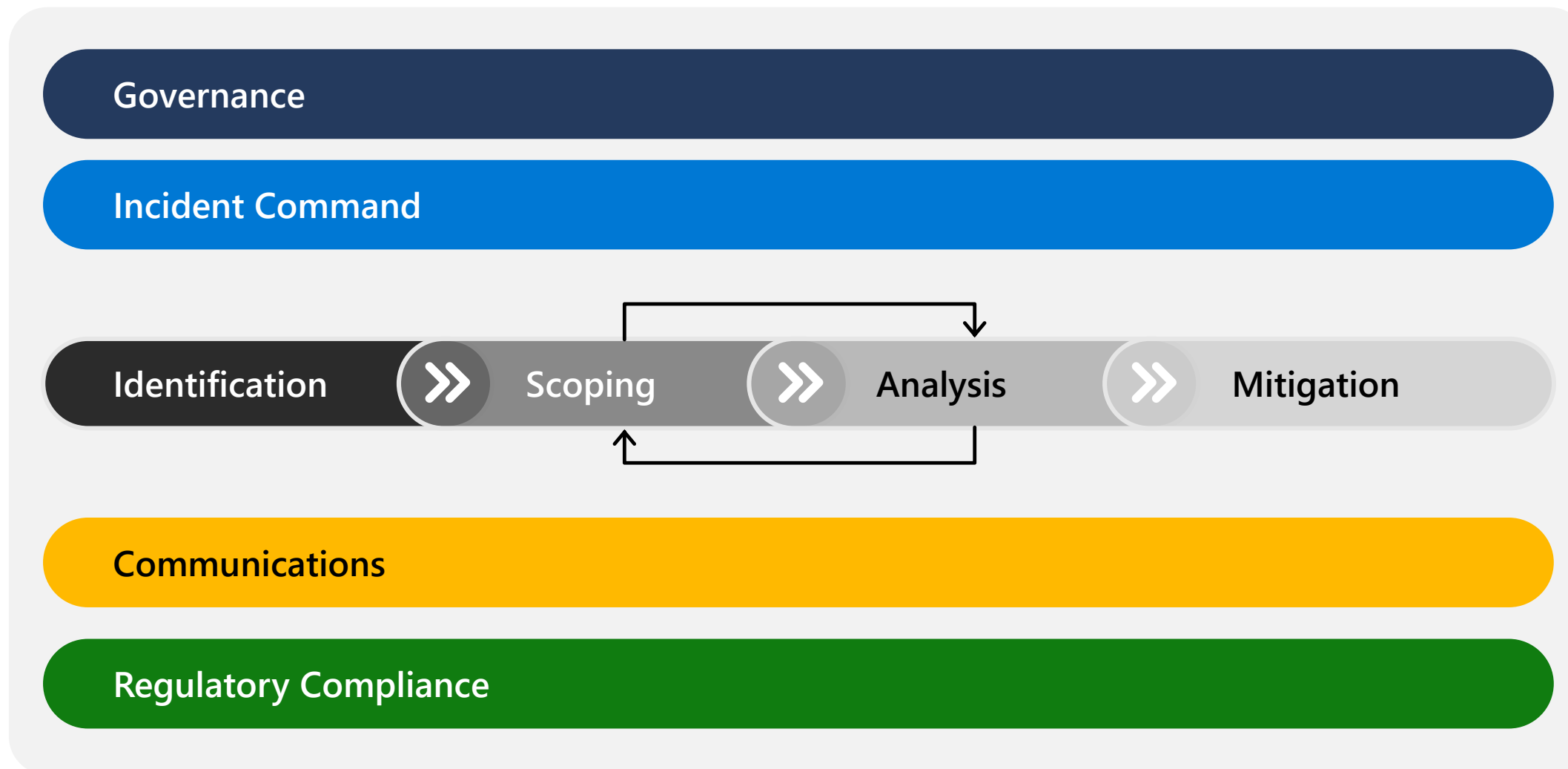
[Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf](#)
[Cyber Resilient Organization Study 2021 | IBM](#)



Incident response methodologies

Both incident management methodologies and the incident response lifecycle are well documented by the [National Institute of Standards and Technology](https://www.nist.gov) (NIST). While there are variations of the lifecycle model, the typical phases include preparation, detection, containment, eradication, recovery, and post-incident activity or lessons learned.

When an organization is caught in a reactive position, we assume it is too late to prepare or develop a comprehensive plan and that lessons learned will be captured following the incident as a long-term incident response plan is developed. In that scenario, let's consider a modified version of these models to help frame up a tactical response plan.



How do you navigate this document?

Home

Click the blue home button to navigate to the at-a-glance map view of the maze, making it easier to plan your next steps.

Role Path

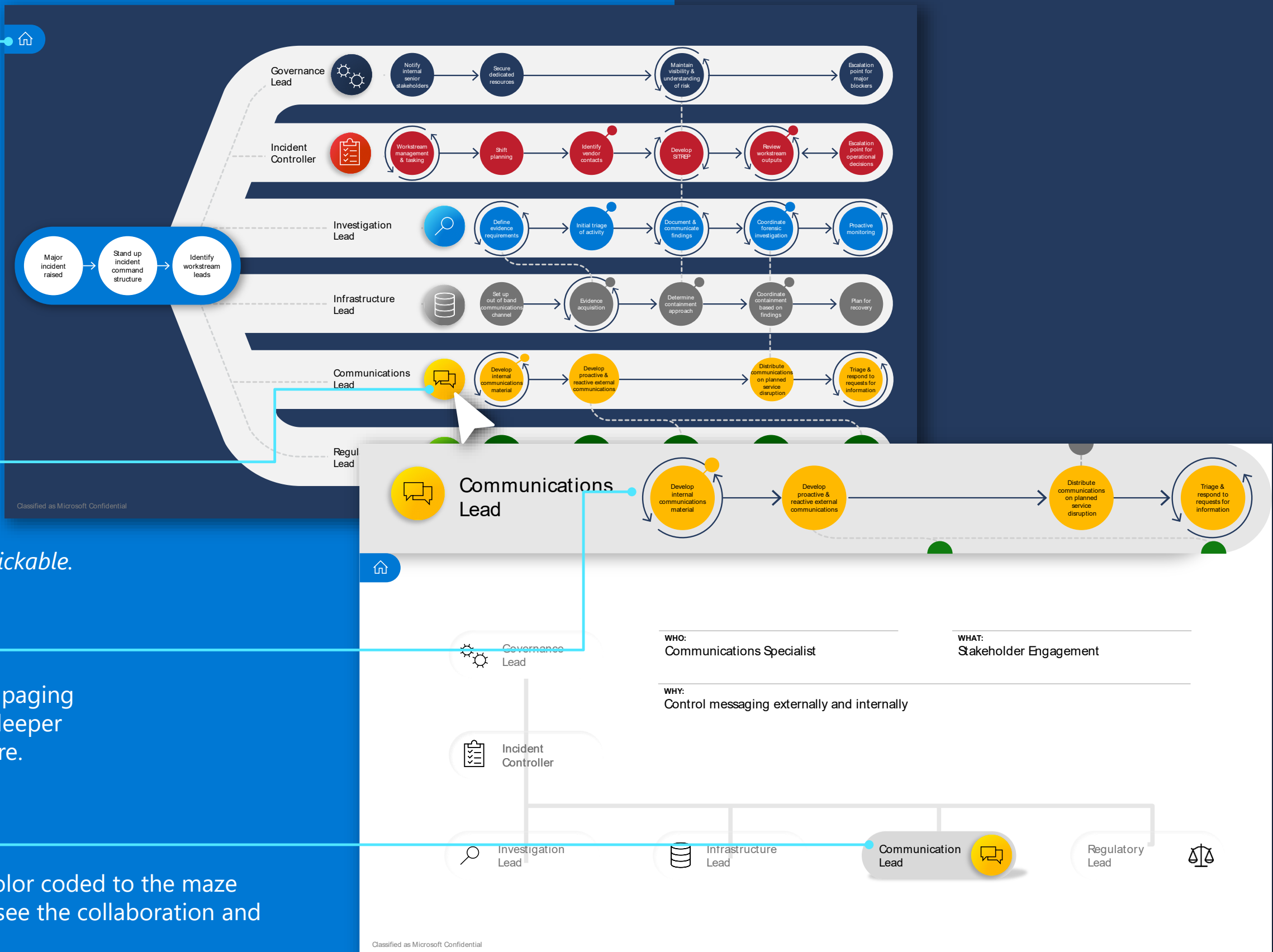
Discover the unique role-based process flow of the response plan by clicking a circle.
Pro Tip: Every circle on the maze map view is clickable.

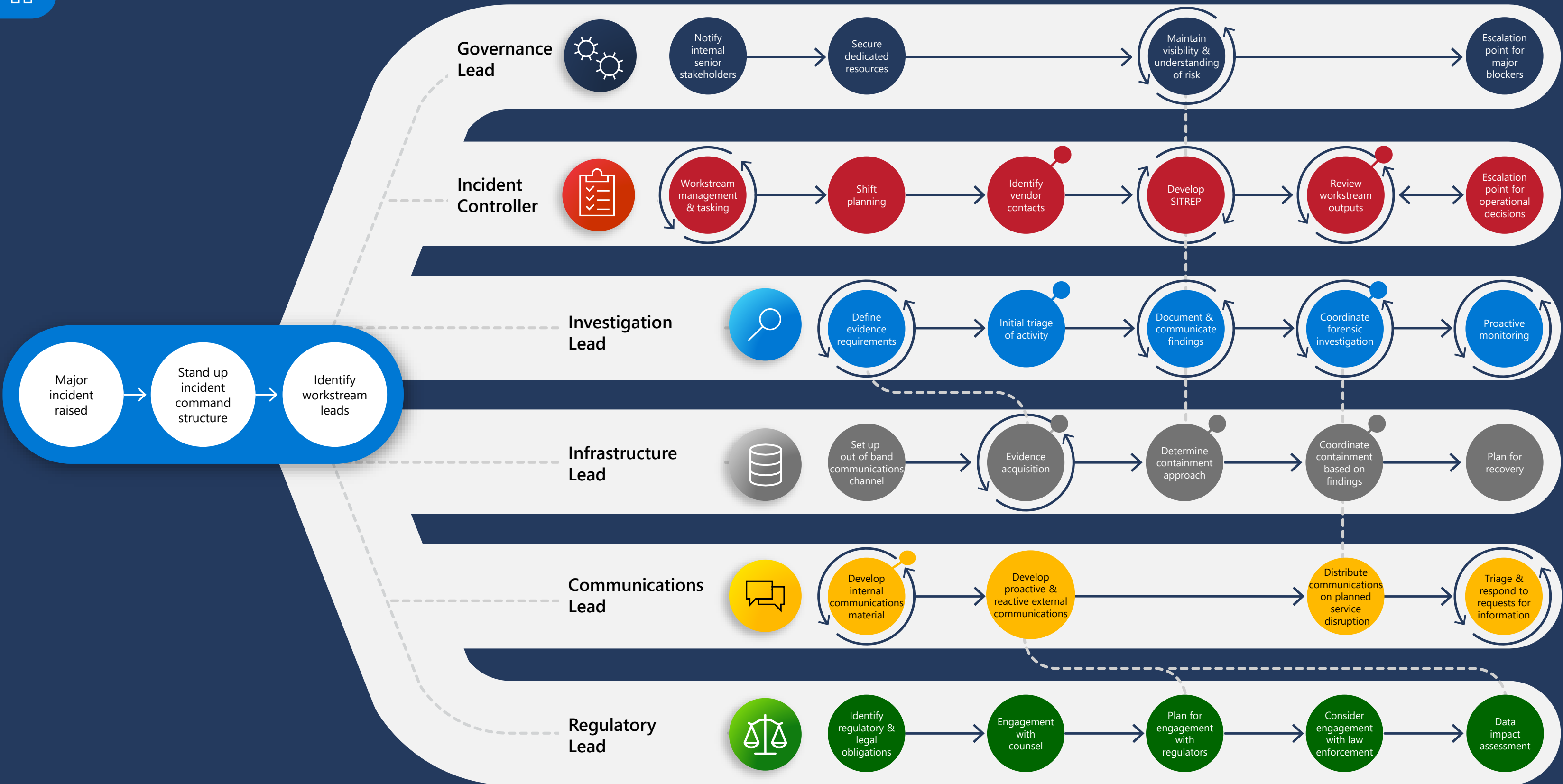
Path Navigation

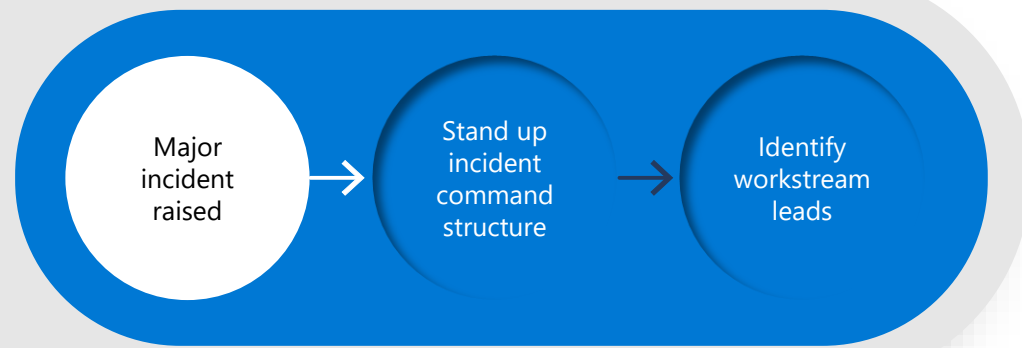
Navigate the steps within the response plan by paging next or by clicking into each segment. To dive deeper into the smaller nodes, simply click to learn more.

Role Hierarchy

The current/activated role is highlighted, and color coded to the maze map. Click to skip around the role hierarchy to see the collaboration and escalation points by clicking a role.





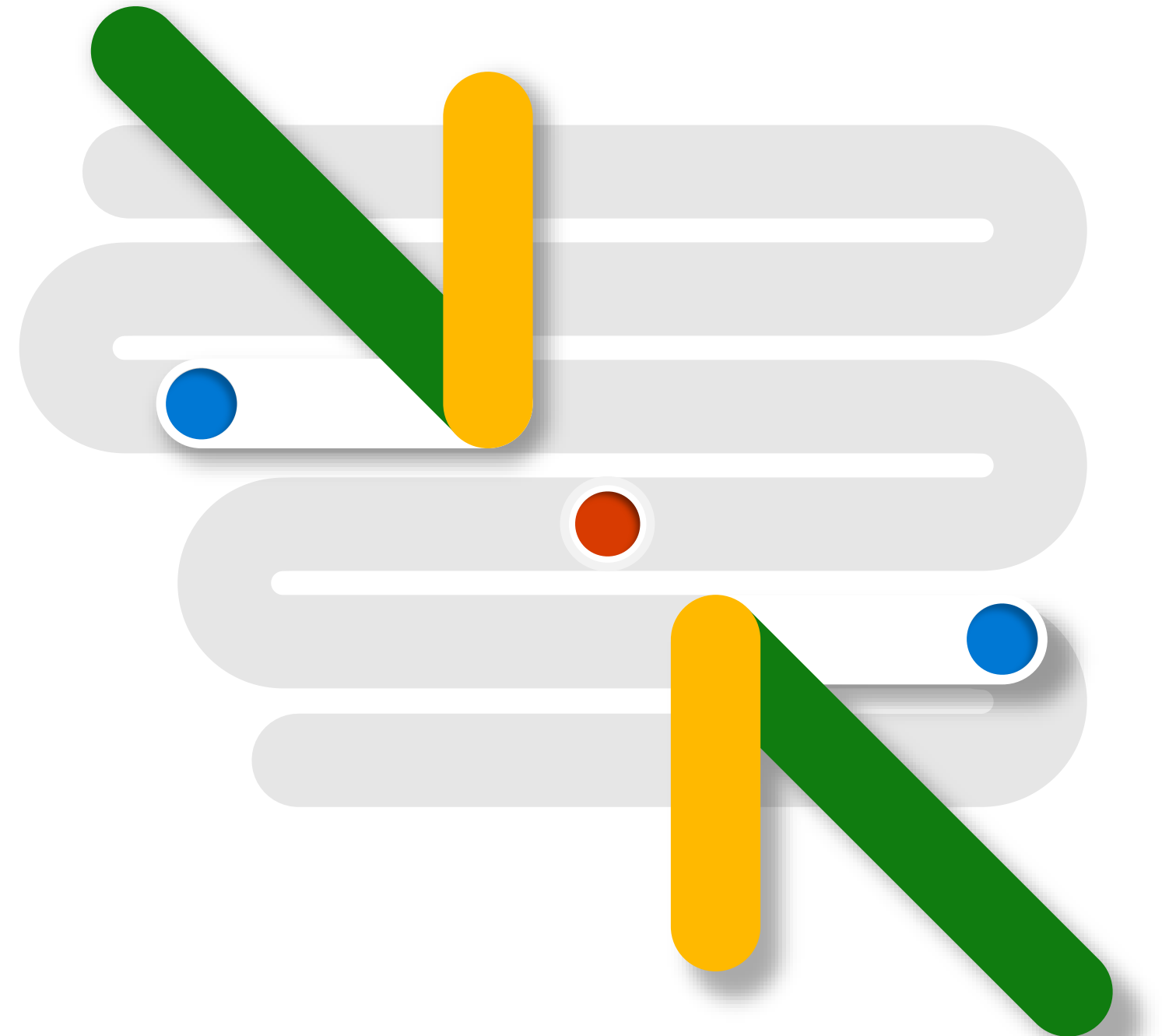


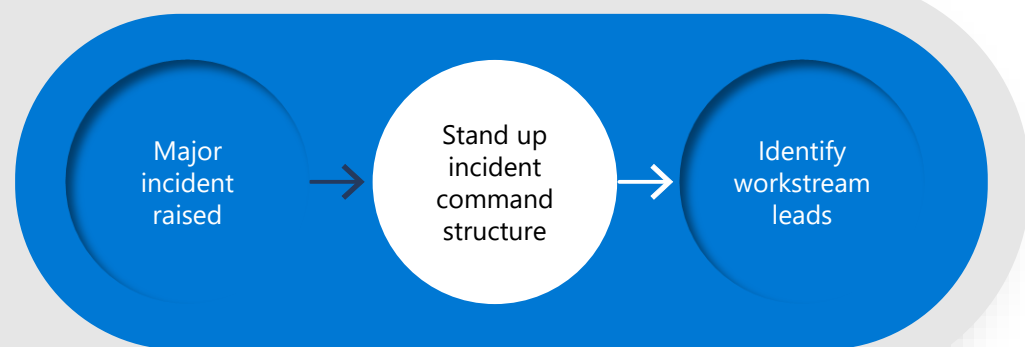
Major incident raised

At the outset of an incident, organizations are typically trying to understand what transpired while grappling with potential business disruption or reputational damage.

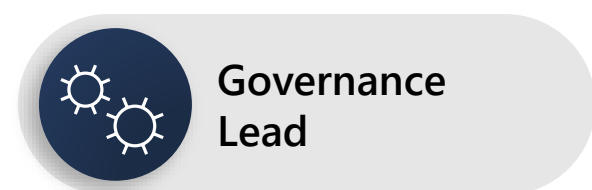
In the absence of a defined incident response plan and command structure, things can be quite chaotic. Operational staff gravitate towards remediating known issues as quickly as possible, often before a comprehensive investigation has been performed. This can lead to ineffective remediation or inadvertent evidence destruction.

To mitigate this, organizations should define a response model to manage the incident.





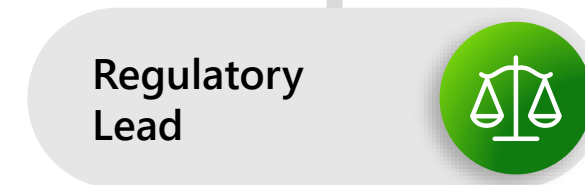
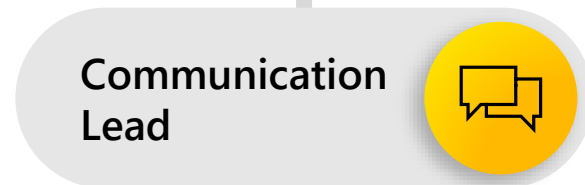
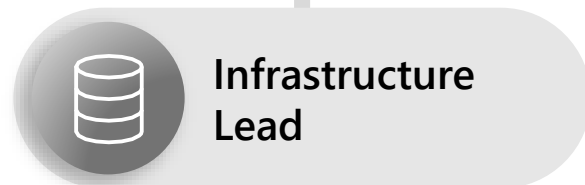
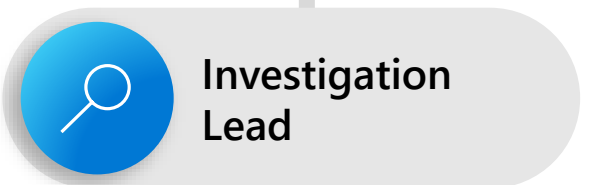
Stand up incident command structure

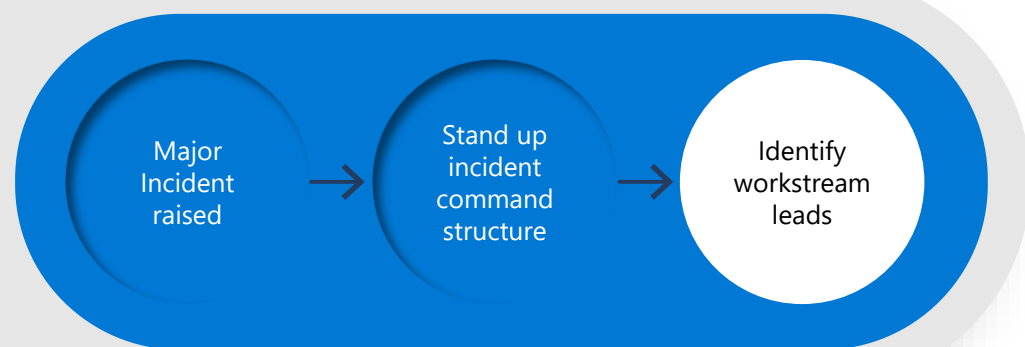


At the leadership level, senior stakeholders are often not privy to the true impact and risk associated with an incident, as communication channels have not been clearly defined. Senior leaders can only make informed decisions about how to manage a response if they are provided with the information needed to understand the risk.

While the technical elements of the response are typically front of mind, responding effectively means having the right people and structure in place to manage operations. It is important to identify key stakeholders who can temporarily step away from response operations, to help frame up a response structure.

Microsoft Incident Response suggests organizations consider the response model outlined here, to help define workstreams, roles, and responsibilities. This is only a starting point, and additional workstreams may be required depending on the context and complexity of each incident.





Identify workstream leads

To help select the right staff to support an incident response, consider the role profiles below and skill matrix outlined on the following slide.

When standing up a command structure, if you identify a gap in skills, consider early engagement with stakeholders to request resourcing support, or plan to engage with a vendor.



Governance Lead

WHO:
CISO/CIO

WHAT:
Operational Oversight

WHY:
Maintain visibility and understand risk and impact to the wider business, communicate with senior stakeholders

Incident Controller

WHO:
ITSM/Security Operations Lead

WHAT:
Operational Management & Tasking

WHY:
Coordinate all operational workstreams to understand and contain the threat. Communicate risk to Governance lead

Investigation Lead

WHO:
Senior IR/Senior IT Operations Rep.

WHAT:
Forensic Investigation

WHY:
Understand the compromise overall and communicate the associated risk

Infrastructure Lead

WHO:
Senior IT Operations Rep.

WHAT:
Threat Containment

WHY:
Contain the threat, reduce risk presented by the compromise

Communications Lead

WHO:
Communications Specialist

WHAT:
Stakeholder Engagement

WHY:
Control messaging externally and internally

Regulatory Lead

WHO:
Internal Counsel/ GRC Rep.

WHAT:
Risk/impact assessment & management of regulatory/legal requirements

WHY:
Maintain compliance

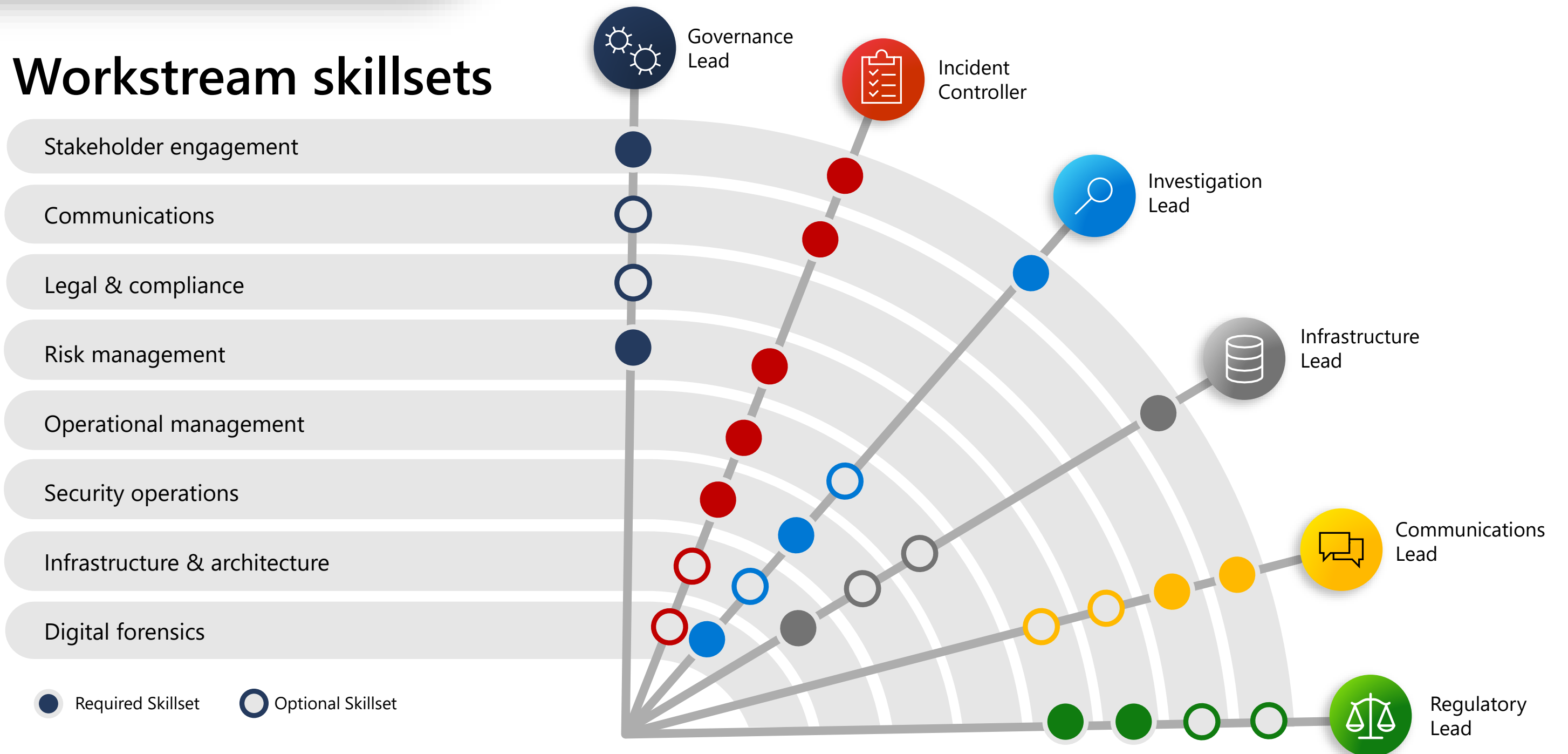


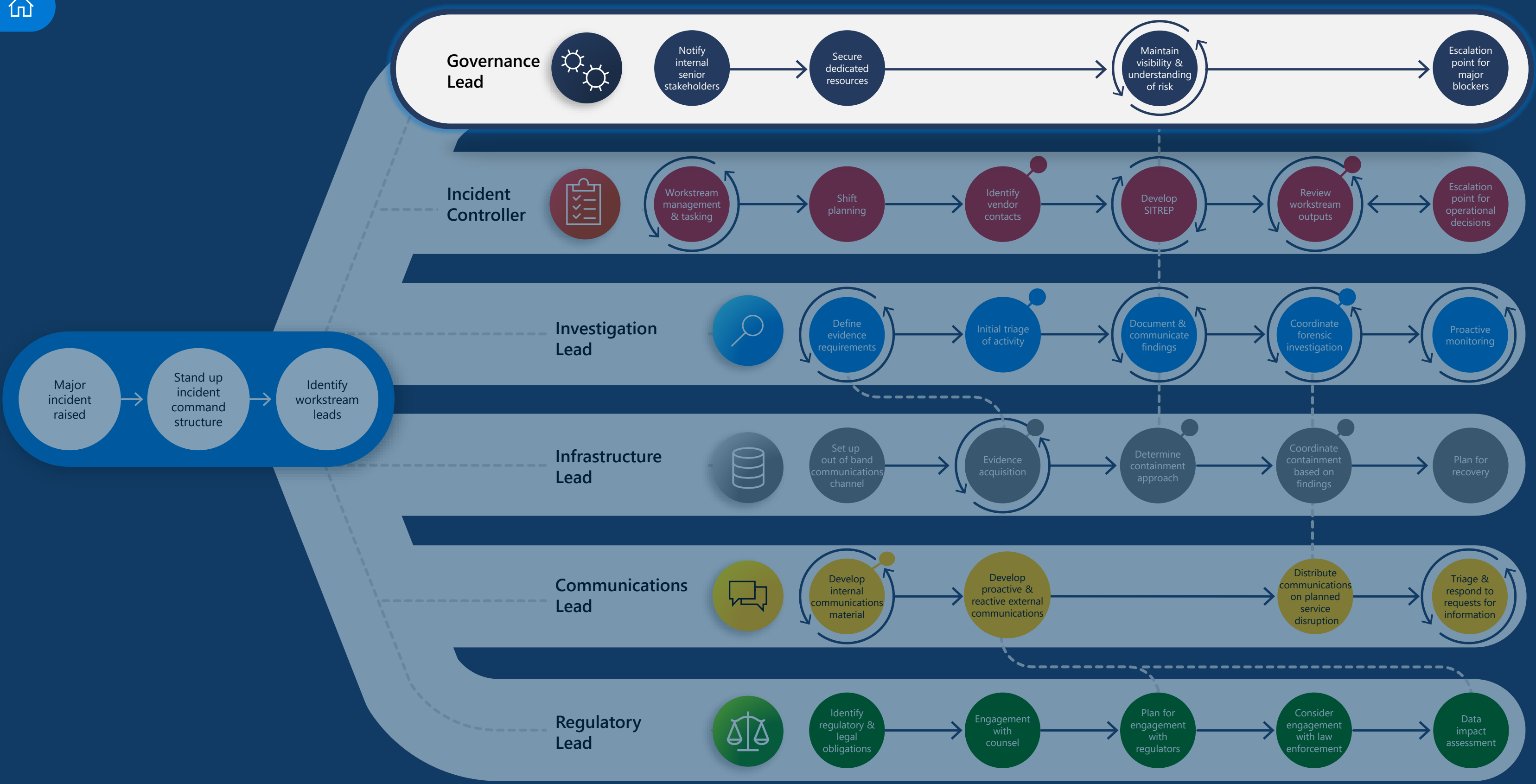
Major incident raised

Stand up incident command structure

Identify workstream leads

Workstream skillsets







Governance Lead


Notify internal senior stakeholders

Secure dedicated resources



Escalation point for major blockers




 Governance Lead

WHO:
CISO/CIO


WHAT:
Operational oversight


WHY:
Maintain visibility & understand risk & impact to the wider business, communicate with senior stakeholders

 Incident Controller

 Investigation Lead

 Infrastructure Lead

Communication Lead 

Regulatory Lead 



Governance Lead



Notify internal senior stakeholders

The Governance Lead should proactively notify senior stakeholders and members of the Executive Leadership team that a major response is underway. This will ensure that other parts of the business are aware of the potential risk and that service disruption may occur while the incident is being managed. Early notification also establishes the Governance Lead as point of contact for all incident-related inquiries from senior stakeholders and mitigates the risk of business units acting themselves.

The Governance Lead should also highlight that requests for support need to be prioritized by other parts of the business.

Common pitfall

If senior stakeholders are not aware of the incident, they may not have the context around why services are unavailable or why containment is required.

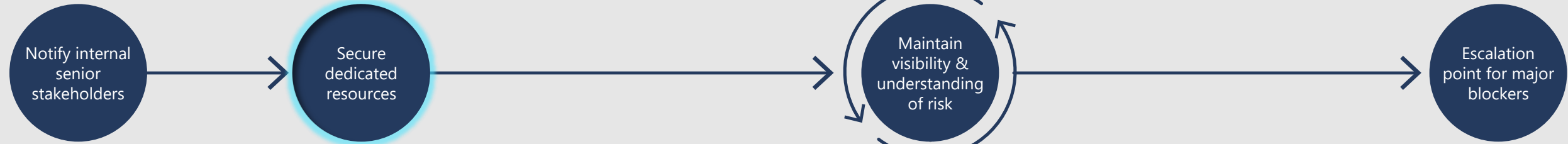
This could lead to other parts of the business independently taking action which reintroduces risk.

If requests for information or support to other parts of the business are not prioritized, this can hinder efficiency as the response team has to escalate requests for support on an ad-hoc basis.



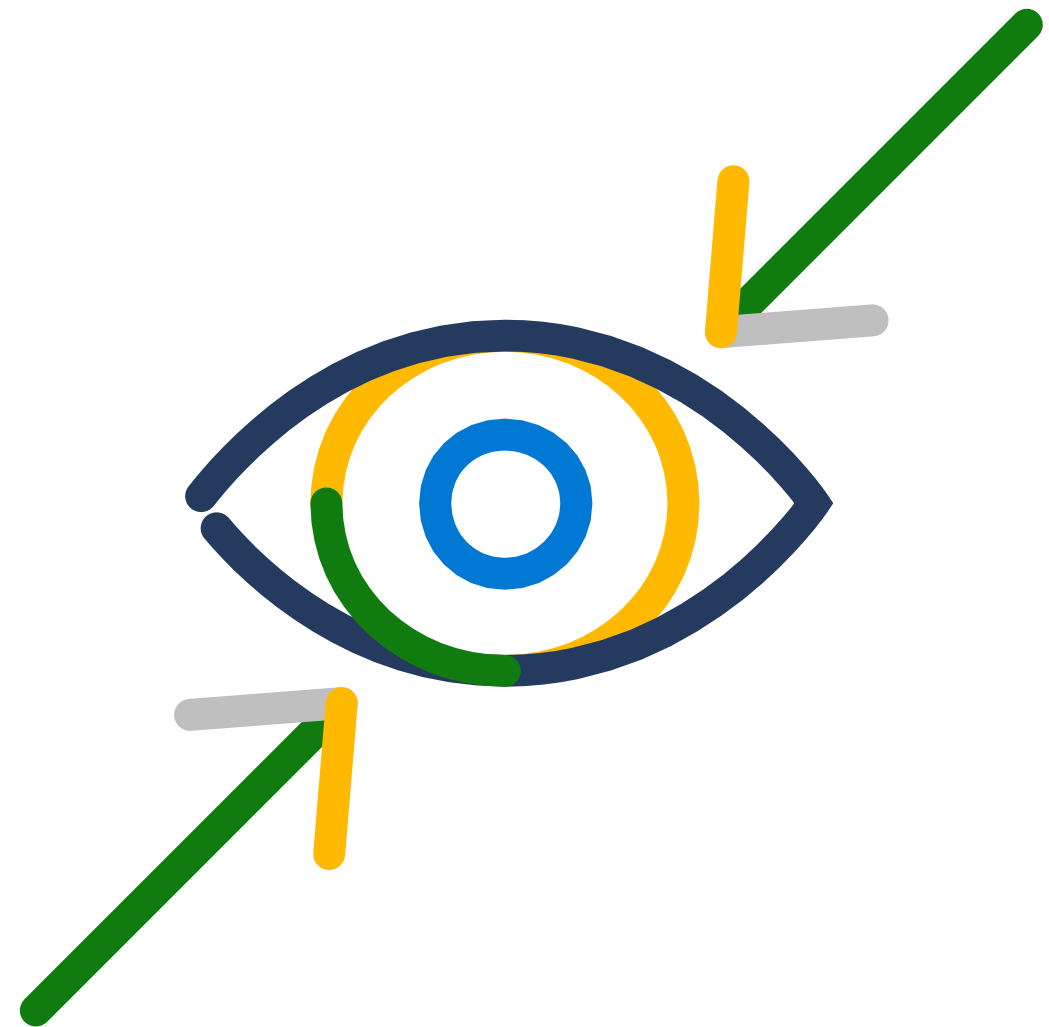


Governance Lead



Secure dedicated resources

Organizations without dedicated security teams often deputize resources from other parts of the business to assist with the response. These individuals then need to balance their existing workload with response activities. Whenever possible, dedicated resources should be assigned to the response, or at a minimum be directed to prioritize response activities over other work.





Governance Lead



Maintain visibility and understanding of risk

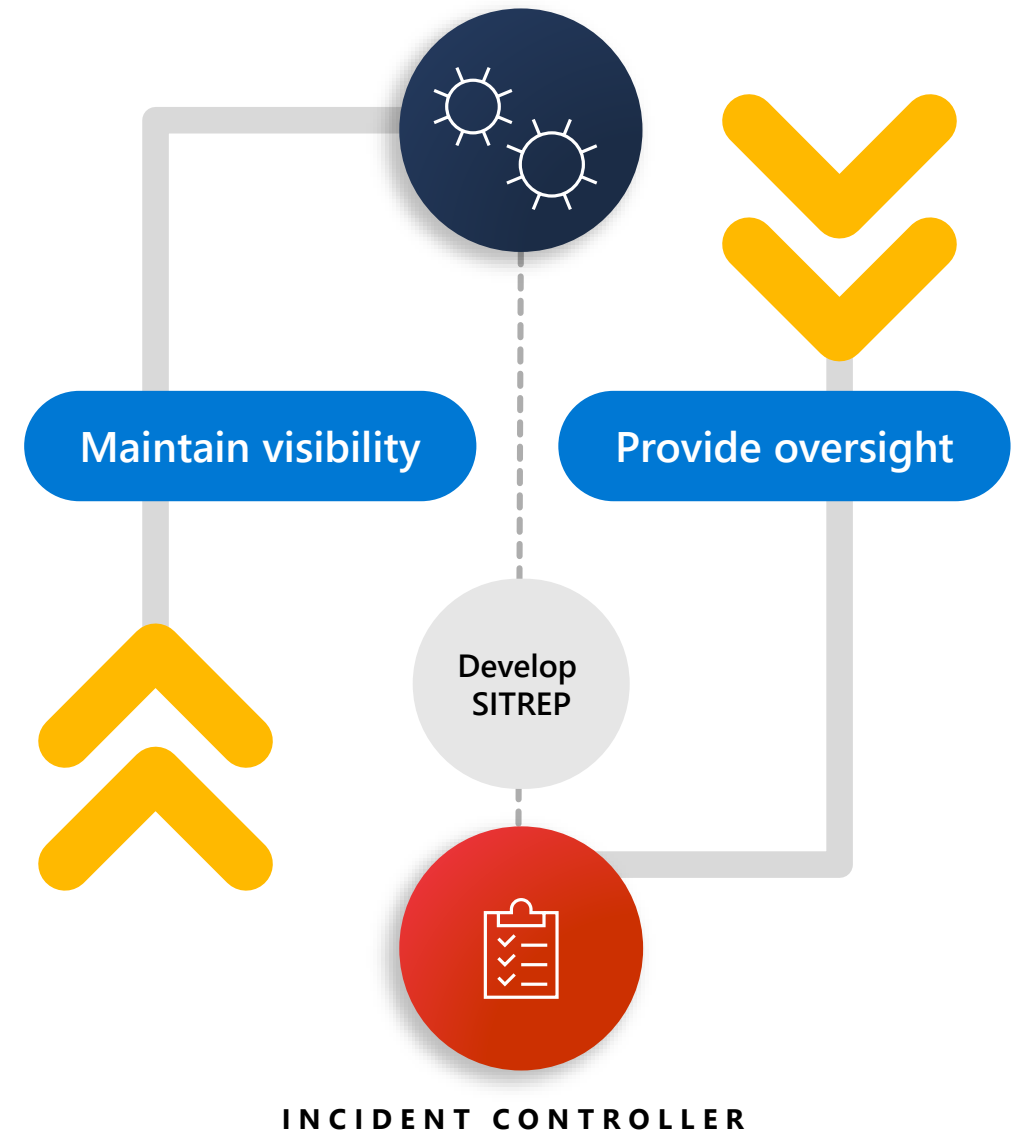
The Governance Lead should maintain oversight of the response to have a clear picture of the risk associated with the incident. This visibility should be maintained throughout the response, via situation reports produced by the Incident Controller.

Common pitfall

At the leadership level, senior stakeholders are often not privy to the true impact and risk associated with an incident, as communication channels have not been clearly defined.

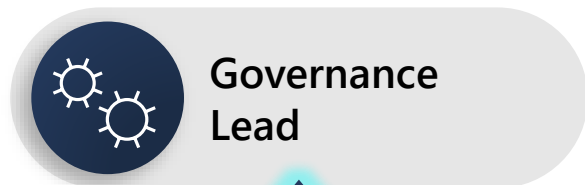
Senior leaders can only make informed decisions about how to manage a response if they are provided with the information they need to understand the risk.

Collaborating role:
[Incident Controller](#) →





Governance Lead



Governance Lead



Incident Controller



Investigation Lead



Infrastructure Lead



Communication Lead



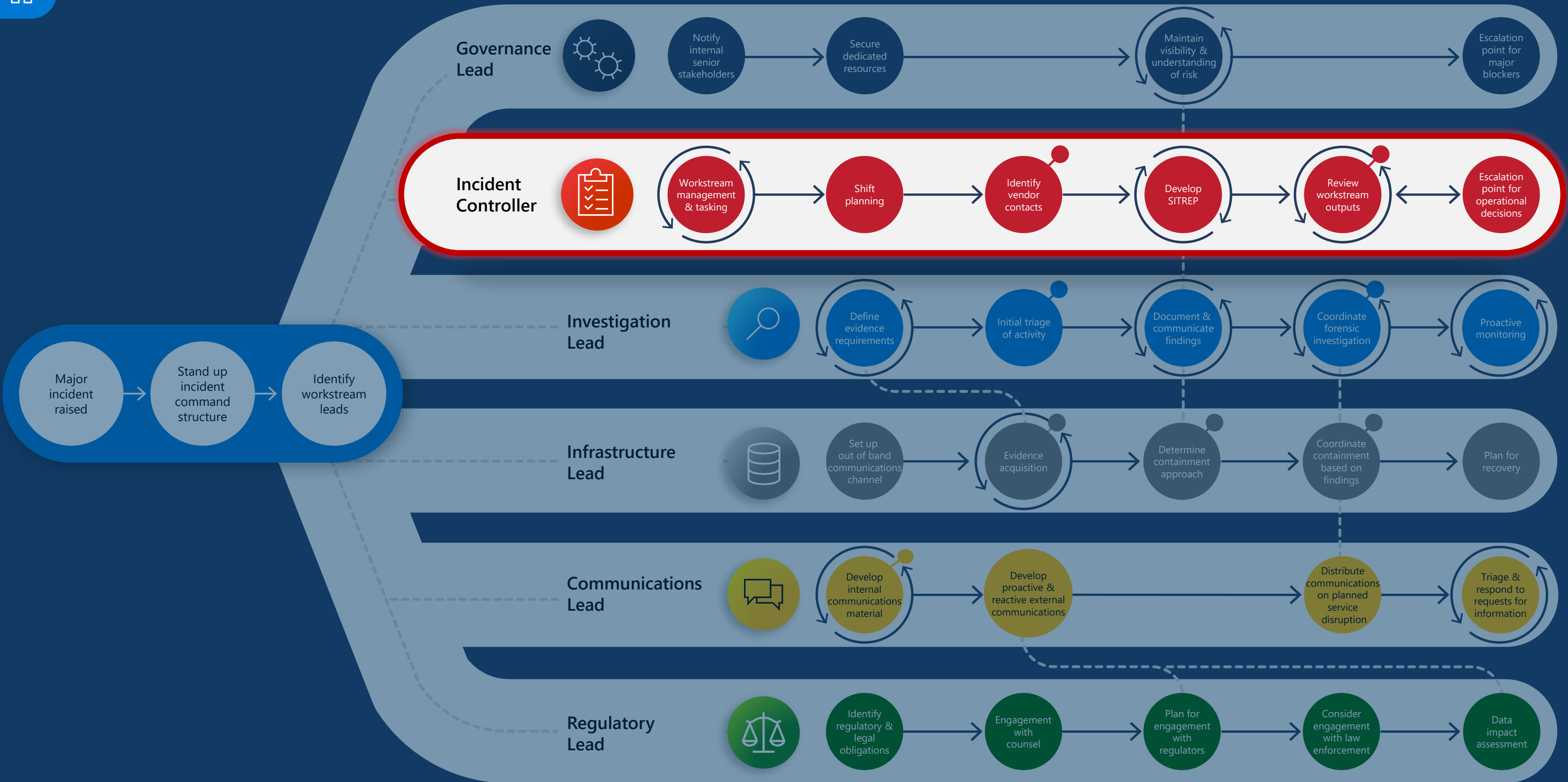
Regulatory Lead

Escalation point for major blockers

The Governance Lead is the response team's interface with both internal and external senior stakeholders. If the response team encounters an issue which cannot be resolved at the operational level, the Governance Lead should provide support.

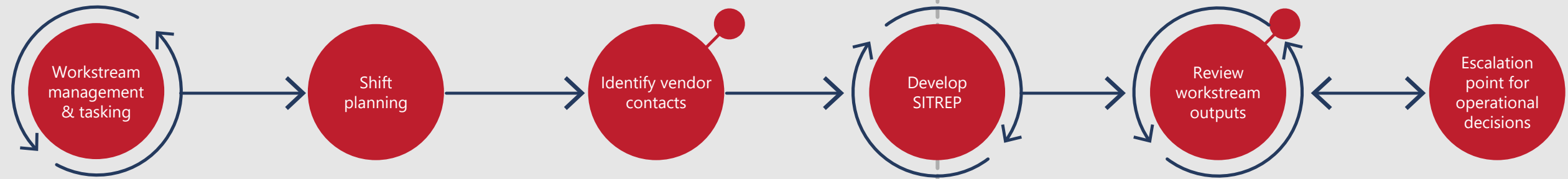
Typical issues which may need support from the Governance Lead include:

- ✓ Resource requests from other parts of the business
- ✓ Escalation of requests to vendors and other third parties
- ✓ Ratify and help to communicate decisions which have wide reaching business impact, such as mass password resets or disabling internet connectivity





Incident Controller



Governance Lead

WHO:
ITSM/Security Operations Lead

WHAT:
Operational management & tasking

WHY:
Coordinate all response streams to understand, contain, and communicate the threat to Governance Lead



Incident Controller



Investigation Lead



Infrastructure Lead

Communication Lead

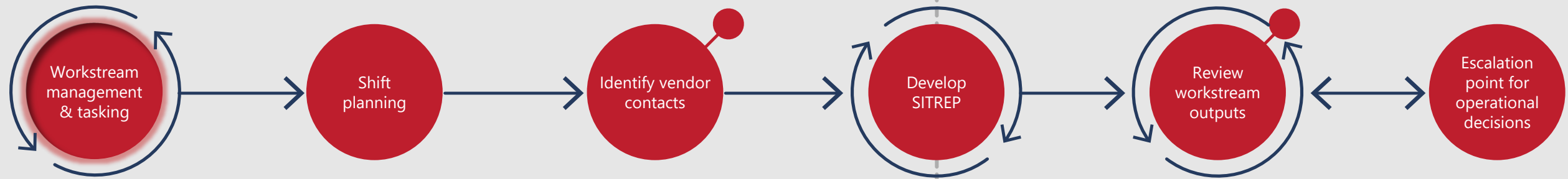


Regulatory Lead





Incident Controller

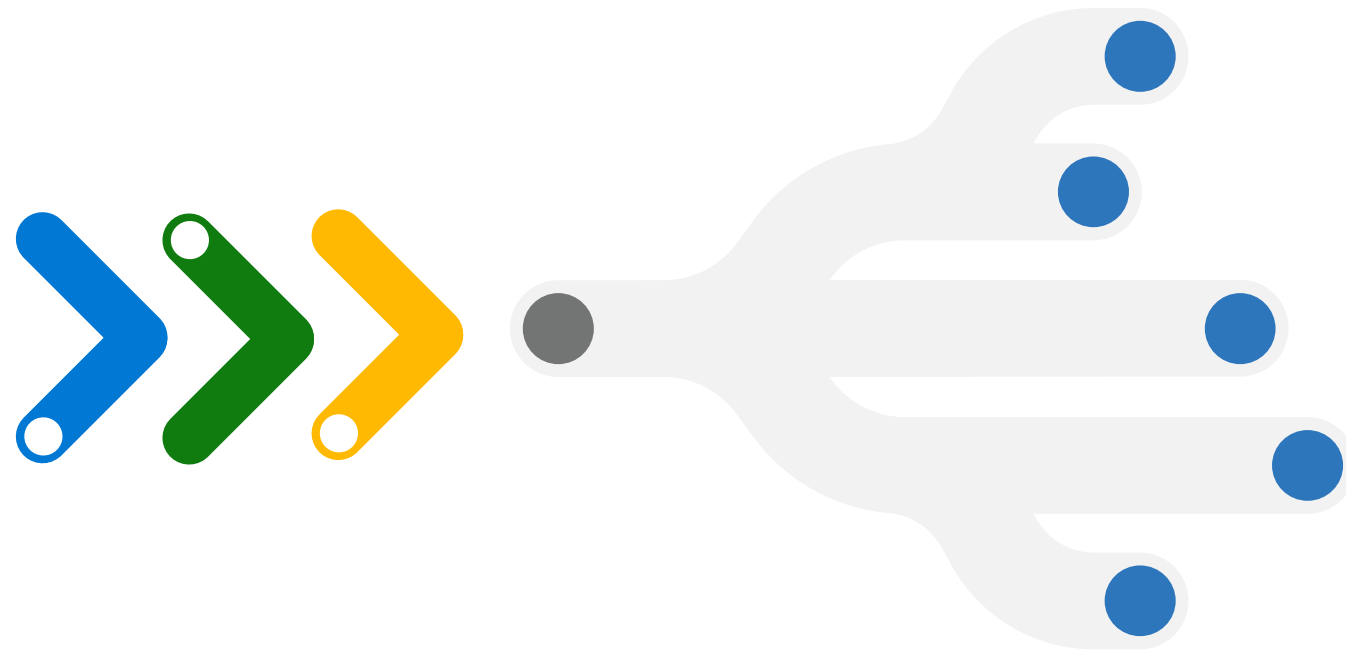


Workstream management and tasking

In the middle of a response, documentation of actions and tasks is often deprioritized in favor of rapid execution. As the response continues, this creates confusion if there isn't a clear record of actions taken and decisions made. The Incident Controller should manage and track tasking for all the operational workstreams to ensure actions are prioritized and that there is a single source of truth on response activities.

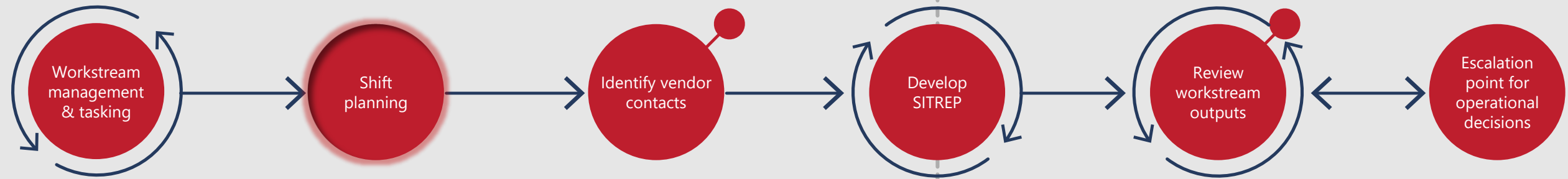
Common pitfall

Lack of documentation can lead to double handling and an inefficient response as the team must back track to determine what was done previously. During a complex response across multiple geographies, this can waste valuable time.





Incident Controller

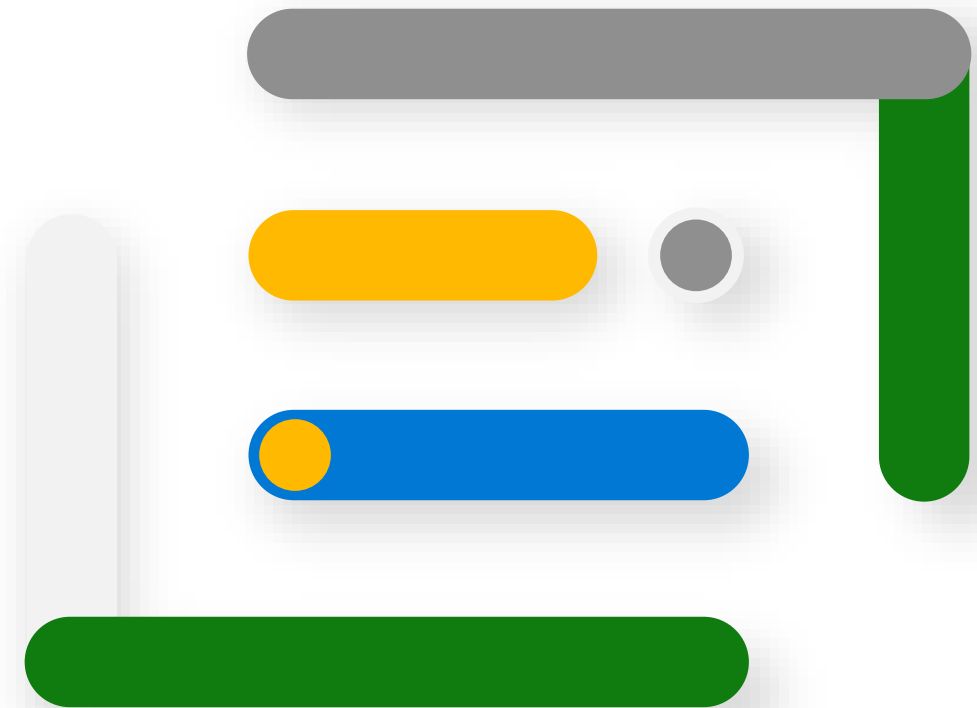


Shift planning

Organizations often require an incident response to run across multiple time zones with coordination across geographically-dispersed business units. In these situations, the response model should define workstream leads for multiple time zones. Shift plans should be clearly defined with set handover meetings to enable a seamless transition between time zones.

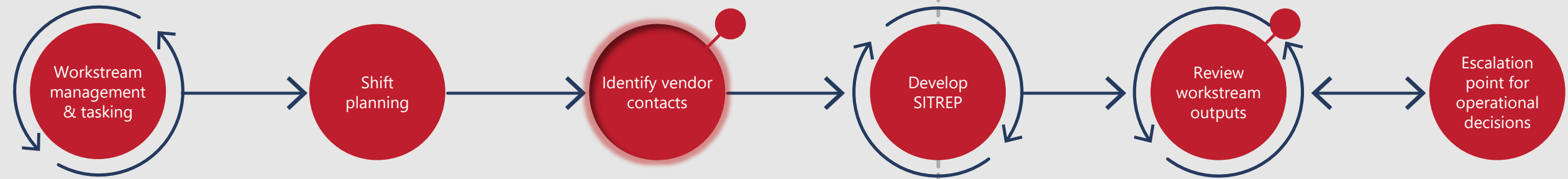
Common pitfall

Resource and shift planning is often overlooked, leading to burn out of key individuals and reduced overall efficiency. Keep in mind that a response operation may extend to weeks or even months.





Incident Controller



Identify vendor contacts

An organization may rely on multiple vendors for IT services or may outsource the entirety of their IT operations. During an incident, engagement with these vendors may be required to support evidence acquisition, containment, and hardening. The Incident Controller should have a clear picture of who these players are so requests can be channeled to the right third party efficiently.

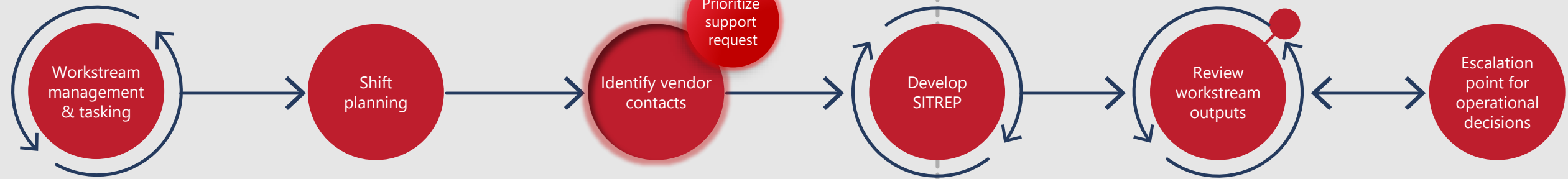
Common pitfall

Lack of proactive engagement and escalation of requests can delay response activities, potentially giving the Threat Actor valuable time to complete their actions on objective.

If vendors are not aware of the situation, containment and hardening actions may be undone as a part of regular support operations.



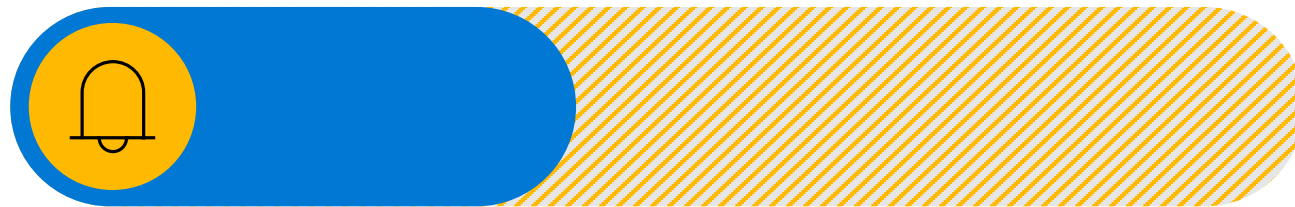
Incident Controller



Identify vendor contacts

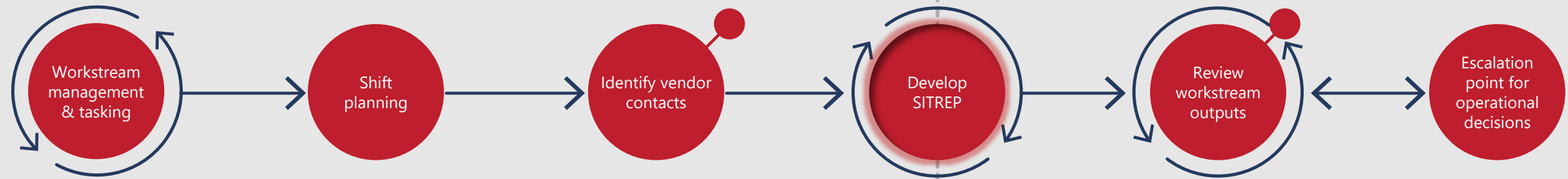
Notify to prioritize support requests

Where possible, proactive engagement with vendors should occur, to ensure that they prioritize requests related to the incident. Do not disclose more information than required to vendors, but leverage account managers or other trusted contacts to ensure they are aware of the urgency.





Incident Controller



Develop SITREP

Situation reports (SITREPs) allow for proactive communication with key stakeholders, ensuring a single source of truth on the risk, as well as an understanding of the actions being taken to investigate and mitigate it. This can help fill the information void and control messaging among internal stakeholders.

At a minimum SITREPs should include:

- ✓ An overview of the workstream leads and their contact details
- ✓ A brief, easily digestible summary of the incident
- ✓ A summary of the key known risks and escalation triggers
- ✓ An action tracker, outlining key tasks in each workstream, their status, and main point of contact
- ✓ A statement outlining when stakeholders can expect the next SITREP

Collaborating roles:

[Governance Lead](#) → [Investigation Lead](#) →

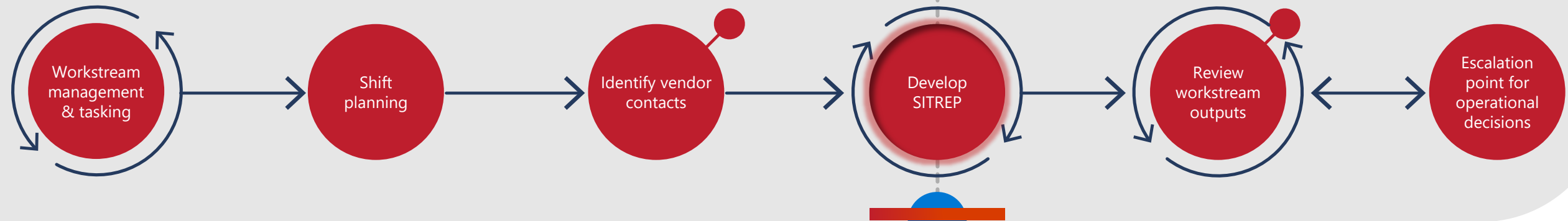
Common pitfall

Often organizations neglect to provide timely updates on progress, choosing to focus on the technical elements of the response. This creates an information void, leading to increased pressure on the Incident Controller and Governance Lead to provide ad-hoc updates to various stakeholders who are concerned about the risk.

SITREPs should remove the need for ad-hoc communications related to the response; if the response team is continually receiving questions, consider more frequent updates or adjusting the distribution list.



Incident Controller



Develop SITREP continued...

Organizations should also consider the cadence and distribution list for SITREPs:



Ensure the cadence of SITREPs matches the severity of the incident.

Typically, SITREPs should be shared daily. But for a less impactful incident, weekly or bi-weekly may be more appropriate.



SITREPs typically contain detailed information about the response. As such, they should only be disseminated to individuals with a "need to know."

The list of recipients should be managed by the Incident Controller.

Common pitfall

To prevent SITREPs from being distributed beyond the intended recipients, consider implementing technical controls.

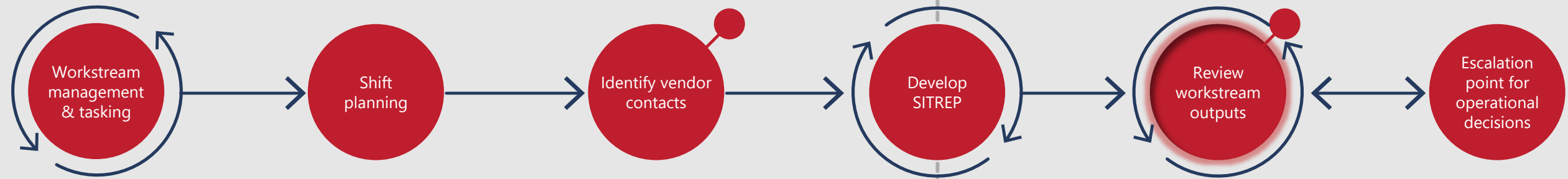
Ensure all recipients are aware that the SITREP is for internal use only, and it should not be used to develop customer-facing communications without consulting the Communications Lead.

Collaborating roles:

[Governance Lead](#) → [Investigation Lead](#) →



Incident Controller

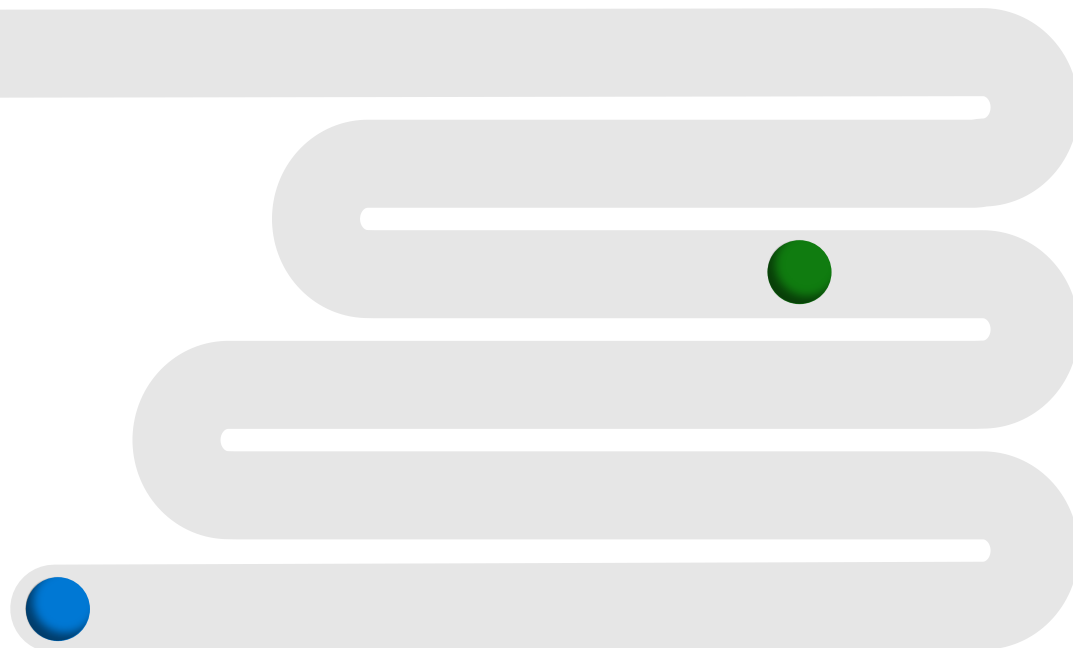


Review workstream outputs

The Incident Controller should have visibility of all workstreams and their outputs to ensure that the response is on the right track and adequately addressing the risk. This enables effective prioritization of tasks and allows for a dynamic approach to be taken.

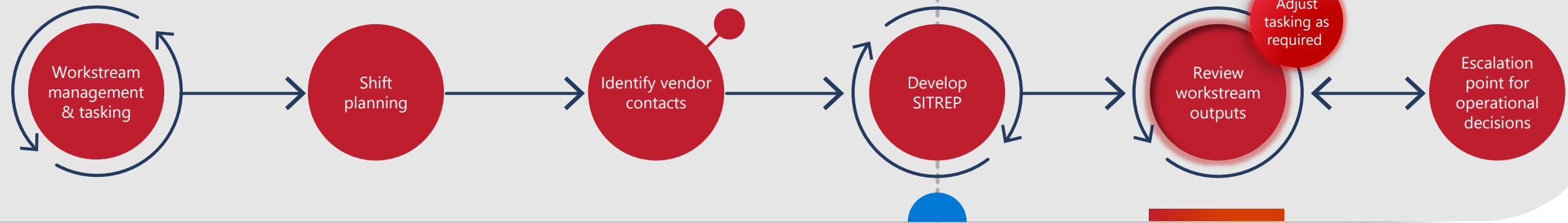
Common pitfall

Often tasking is passed to technical leads, who then delegate tasks to the appropriate staff. If there is no feedback loop, the Incident Controller cannot prioritize tasking effectively and may not be sighted to operational blockers.



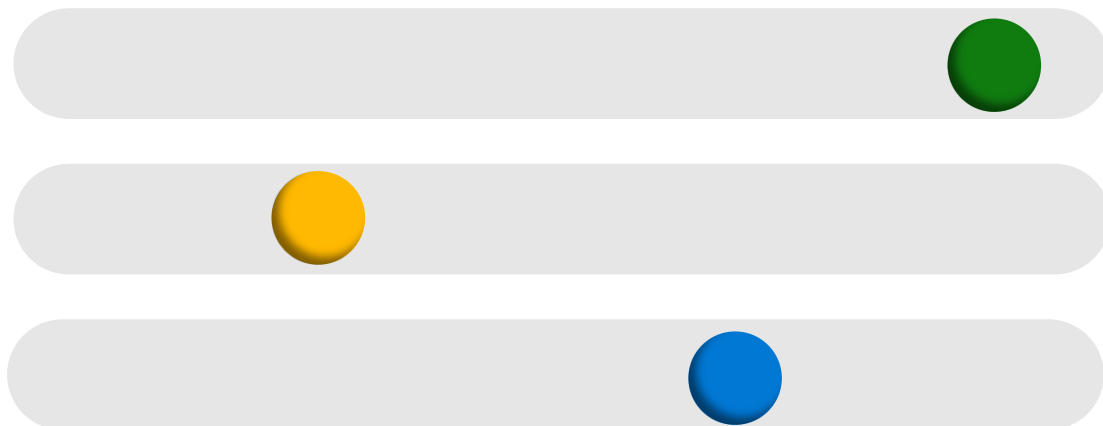


Incident Controller



Adjust tasking as required

The incident response process by nature is dynamic. The workstreams defined in the response model require a high degree of collaboration between all parties. The Incident Controller should have oversight of all operational workstreams and may need to adjust tasking based on workstream output or in response to actions taken by the Threat Actor.



Common pitfall

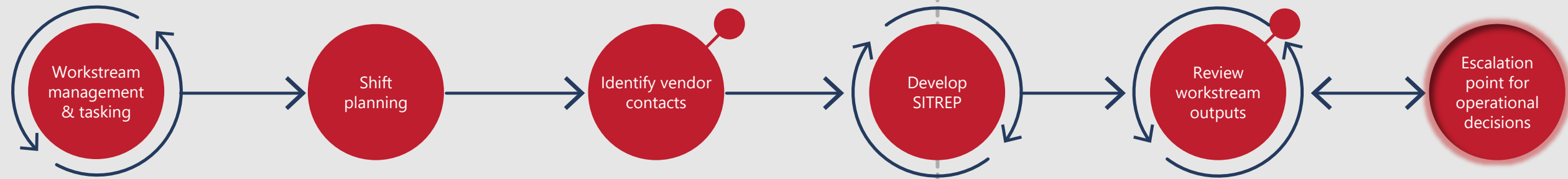
Silos can develop during an incident response, particularly for organizations that are dispersed geographically.

Without oversight of the workstreams and a central point of control, tasking cannot be adjusted and prioritized effectively.

Consider a scenario where findings from the Investigation Lead's workstream are produced in one region, identifying the need for containment of a host. The containment action will be delivered through the Infrastructure Lead's workstream, based in a different region. The Incident Controller must maintain visibility so tasking can be coordinated appropriately.



Incident Controller



Governance Lead

Escalation point for major blockers



Incident Controller

Escalation point for operational decisions



Investigation Lead



Infrastructure Lead

Communication Lead



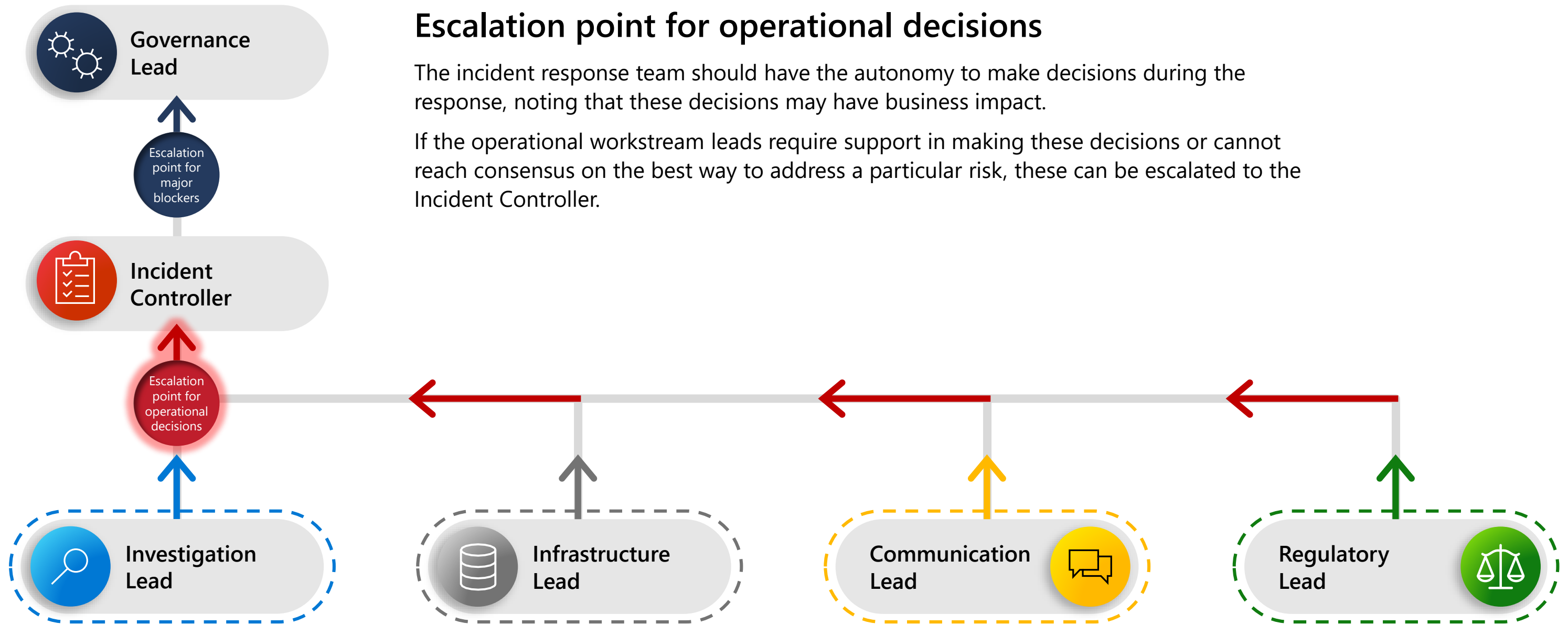
Regulatory Lead

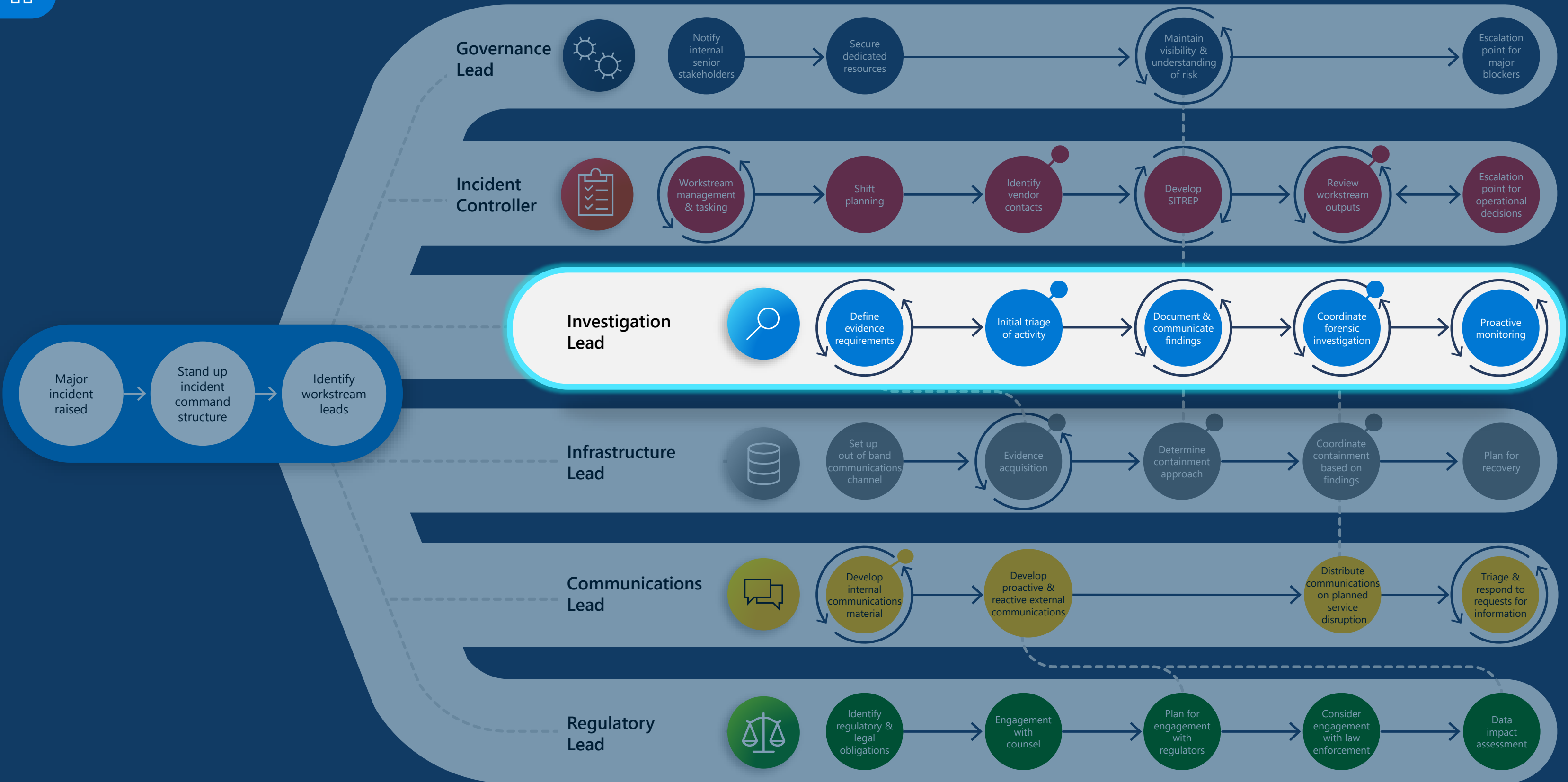


Escalation point for operational decisions

The incident response team should have the autonomy to make decisions during the response, noting that these decisions may have business impact.

If the operational workstream leads require support in making these decisions or cannot reach consensus on the best way to address a particular risk, these can be escalated to the Incident Controller.







Investigation Lead



Governance Lead

WHO:
Senior IR/Senior IT Operations

WHAT:
Forensic Investigation

WHY:
Understand the compromise overall and communicate the associated risk



Incident Controller



Investigation Lead



Infrastructure Lead

Communication Lead



Regulatory Lead





Investigation Lead



Define evidence requirements

When responding to an incident, understanding what occurred is key to ensuring the risk can be mitigated effectively. To enable a comprehensive investigation and develop a full picture of what transpired, evidence preservation and collection must be prioritized.

Approach evidence collection in a tactical and scalable manner. It's not always practical to gather full disk images from every impacted host. Gather only the evidence that is required to help you quickly paint a picture of what the Threat Actor did.

Common pitfall

Often recovery efforts are prioritized, and hosts are rebuilt before forensic evidence can be collected.

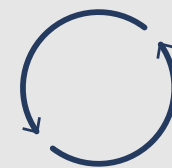
As a result, key pieces of intrusion timeline remain undiscovered, leaving the organization vulnerable to similar incidents in future.

>> Historical Data

>> Live Data

>> Contextual Data

On-Premises



Cloud



Historical Data >>

Live Data >>

Contextual Data >>

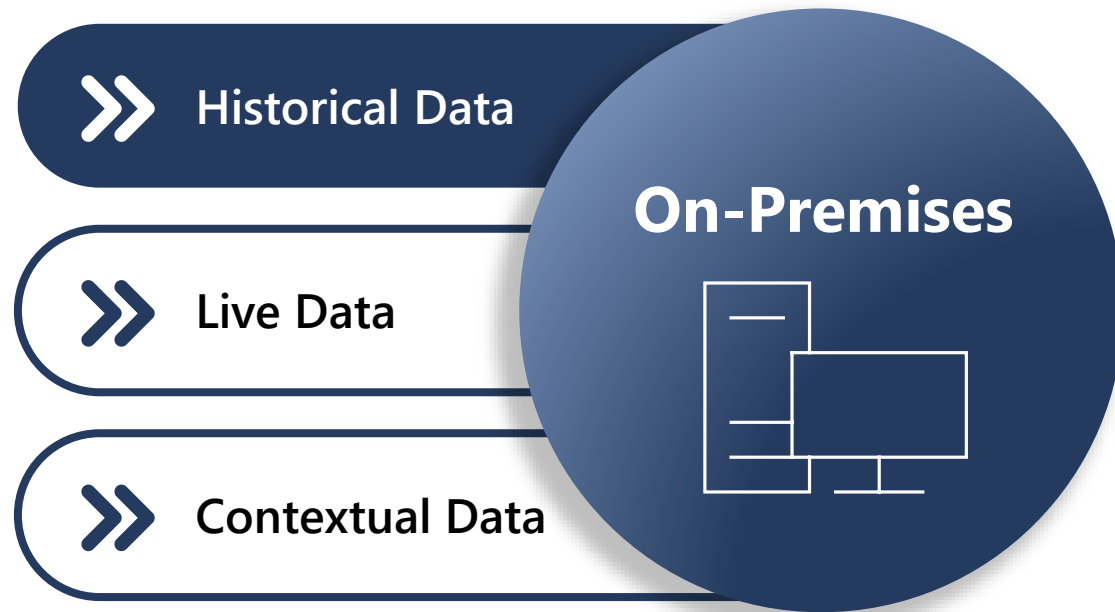


Investigation Lead



Define evidence requirements

EVIDENCE TYPE: Historical Data



✓ Triage Images

A triage image allows for scalable collection and efficient analysis of select artifacts from impacted devices; key logs and forensic artifacts can be captured from hosts, negating the need for full disk image analysis.

✓ Disk Images

A full disk image may be required to collect more abstract artifacts when dealing with a more sophisticated attack where defense evasion or novel tactics, techniques, and procedures (TTPs) are employed.

✓ Memory Images

May be required for deeper analysis of key hosts where novel malware or TTPs are employed by the actor, which do not leave evidence on disk.

Collaborating role:
[Infrastructure Lead](#) →



Investigation Lead



Define evidence requirements

» Historical Data

» Live Data

» Contextual Data

On-Premises



EVIDENCE TYPE:

Live Data

✓ EDR Monitoring

If an endpoint detection and response (EDR) product is not deployed already, it should be prioritized at the outset of an incident to ensure full visibility of ongoing activity within the network.

✓ Active Blocking or Auditing

Blocking mode is recommended regardless of the incident, along with a robust process to triage and deconflict block events as they occur.

This enables analysts to perform real-time interdiction of further malicious activity.

✓ Custom Alerting

Analysts should be provided with the ability to add custom indicators and detections as analysis progresses.

Collaborating role:
[Infrastructure Lead](#) →



Investigation Lead



Define evidence requirements

» Historical Data

» Live Data

» Contextual Data

On-Premises



EVIDENCE TYPE:

Contextual Data

✓ Boundary Device Logging

Network logging should be interrogated to understand how the Threat Actor was able to access the network remotely.

Consider analysis of boundary devices such as firewalls, VPN appliances, proxies, and internet exposed web servers.

✓ Centralized SIEM

It is best practice to ensure key logs from across an environment are centralized in a SIEM solution.

✓ Remote Access Architecture

This is key when paired with the Boundary Device Logging; analysts must know how traffic will flow through a network to understand what logging to request and what types of indicators are relevant.

Collaborating role:
[Infrastructure Lead](#) →



Investigation Lead

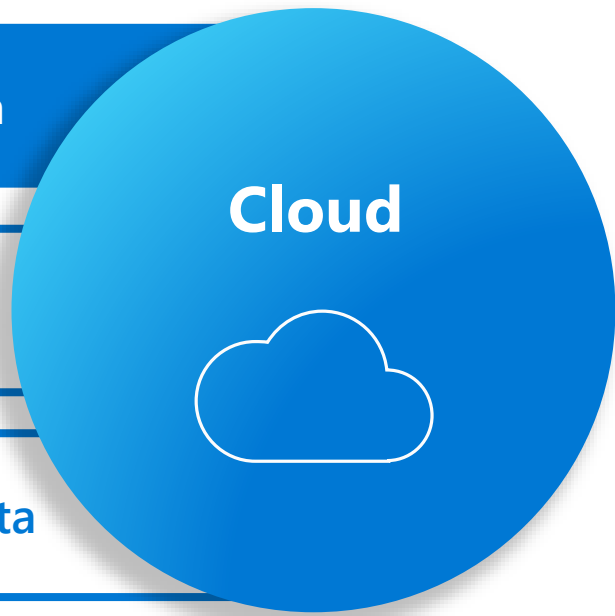


Define evidence requirements

» Historical Data

» Live Data

» Contextual Data



Collaborating role:
[Infrastructure Lead](#) →

EVIDENCE TYPE: Historical Data

✓ Sign-in & Audit Logging

Sign-in data and administrative actions undertaken by compromised identities are the cornerstone of analysis in the cloud.

If not centralized, this logging is only available for the past 30 days in Microsoft security portals (may vary for other cloud platforms).

✓ Application & Activity Logging

Non-human identities and actions taken in cloud workloads should be scrutinized just as closely as those tied to traditional users.

If not centralized, this logging is only available for the past 30 days in Microsoft security portals (may vary for other cloud platforms).

✓ Cloud Resource Artifacts

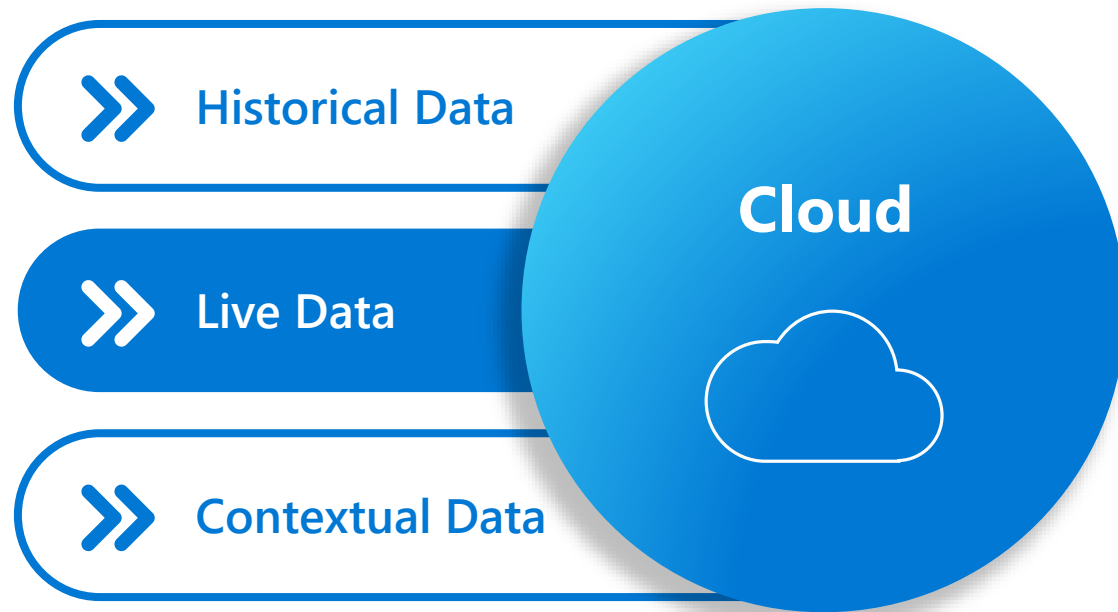
Preservation of evidence in the cloud follows the same principal as that of on-premises; ensure resources are isolated but not deleted as they are identified. Once these artifacts are deleted, they may not be recoverable.



Investigation Lead



Define evidence requirements



EVIDENCE TYPE: Live Data

✓ Identity & Email Provider Alerting

Many identity and email platforms have alerting functionality backed by algorithms to identify anomalous activity (such as Microsoft Entra ID Identity Protection).

✓ Custom Alerting: Sign-in Events

Sign-in events for compromised identities—whether they are successful or failed—should be scrutinized closely for additional indicators or signs of re-compromise.

✓ Custom Alerting: Admin Audit Logs

As the investigation begins and activities undertaken by the Threat Actor are identified, recurring queries and alerting mechanisms should be created to identify additional instances of those actions.

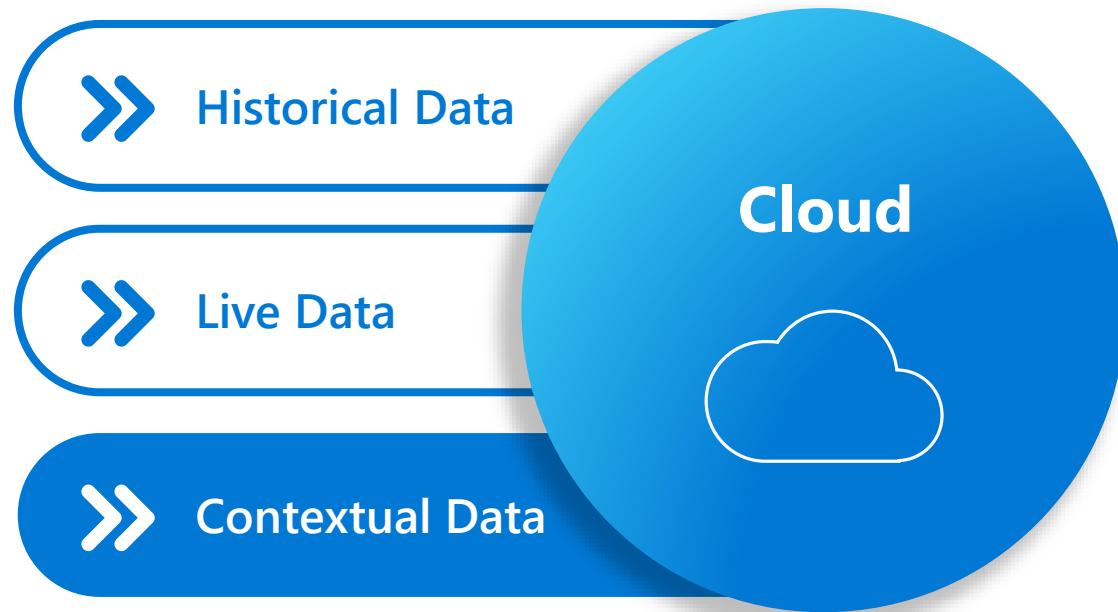
Collaborating role:
[Infrastructure Lead →](#)



Investigation Lead



Define evidence requirements



EVIDENCE TYPE: Contextual Data

✓ Auth & Email Flow Architecture

Understanding the authentication and email flows is key to understanding what logging sources have utility in the content of the investigation.

✓ Centralized SIEM

It is best practice to ensure key logs from across an environment are centralized in a SIEM solution. This enables interrogation of logging from a variety of sources.

✓ Hybrid Architecture

Understanding where the boundaries between on-premises and cloud exist is key to understanding what artifacts need to be collected and what may be targeted by a Threat Actor attempting to maintain a foothold.

Collaborating role:
[Infrastructure Lead →](#)



Investigation Lead



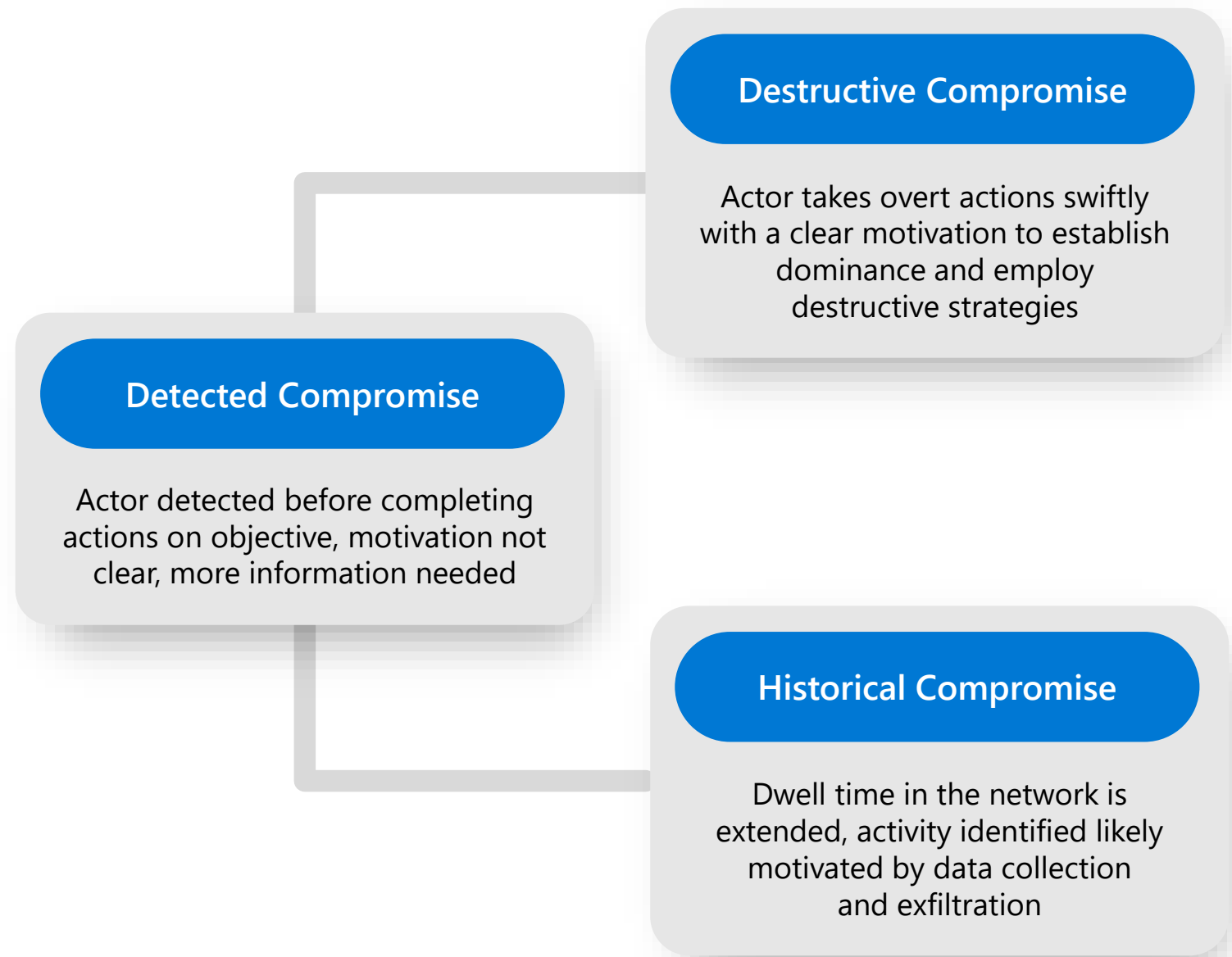
Initial triage of activity

To respond to an incident effectively, an initial triage of the malicious activity which triggered the incident must be performed.

Every incident is unique but can be broadly placed into three Incident Type categories, outlined in the diagram. It is important to understand the context of the incident as this will affect how investigation and containment actions are prioritized.

Generally, every incident begins as a 'Detected Compromise' – malicious activity has been identified, but the motivations and full scope of what the Threat Actor has achieved are unknown.

While the investigation is still in flight, it may be difficult to assess the type of incident being managed. Continually re-assess the situation based on the evidence available to ensure that the approach can be adjusted to manage the risk effectively.





Investigation Lead



Initial triage of activity

Scoping

Triaging the initially detected activity allows for an initial scope of the incident to be determined. As the investigation progresses and findings are developed, the scope of the incident will likely change. This in turn will affect the other workstreams. For example, containment actions may need to be widened to a greater range of hosts or in different domains, and communications material may need to be developed for a broader tranche of customers.

It is imperative that the scope of the incident be continually re-evaluated and understood across the response team as a whole to ensure that response activities can be prioritized to address the risk.

Investigation Findings

Dependent on **Scope** and **Evidence Collection**

Incident Type

Dependent on **Investigation Findings**

Containment Approach

Dependent on **Incident Type**

Containment Steps

Dependent on **Containment Approach**





Investigation Lead



Initial triage of activity

Scoping

Scoping of the incident to determine the Incident Type will help to understand the containment approach that needs to be taken.

Collaborating role:
[Infrastructure Lead](#) →

INCIDENT TYPE

Historical Compromise

Dwell time in the network is extended, activity identified likely motivated by data collection, and exfiltration

Detected Compromise

Actor detected before completing actions on objectives, motivation not clear, more information needed

Destructive Compromise

Actor takes overt actions swiftly with a clear motivation to establish dominance and employ destructive strategies

CONTAINMENT STEPS

Conservative

Prioritize scoping and investigation of compromise before containment

Undertake containment following the investigation, default action to monitor

Strong consideration should be given to impact of containment actions on business operations

Moderate

Prioritize containment of persistence mechanisms, impacted identities, and devices

Undertake containment actions based on continuous risk assessment, default action to block

Moderate consideration should be given to impact of containment actions on business operations

Aggressive

Prioritize containment of tier-0 assets, identities, and remote access solutions

Undertake containment actions in near real time, default action to block

Limited consideration for impact of containment actions on business operations



Investigation Lead



Document and communicate findings

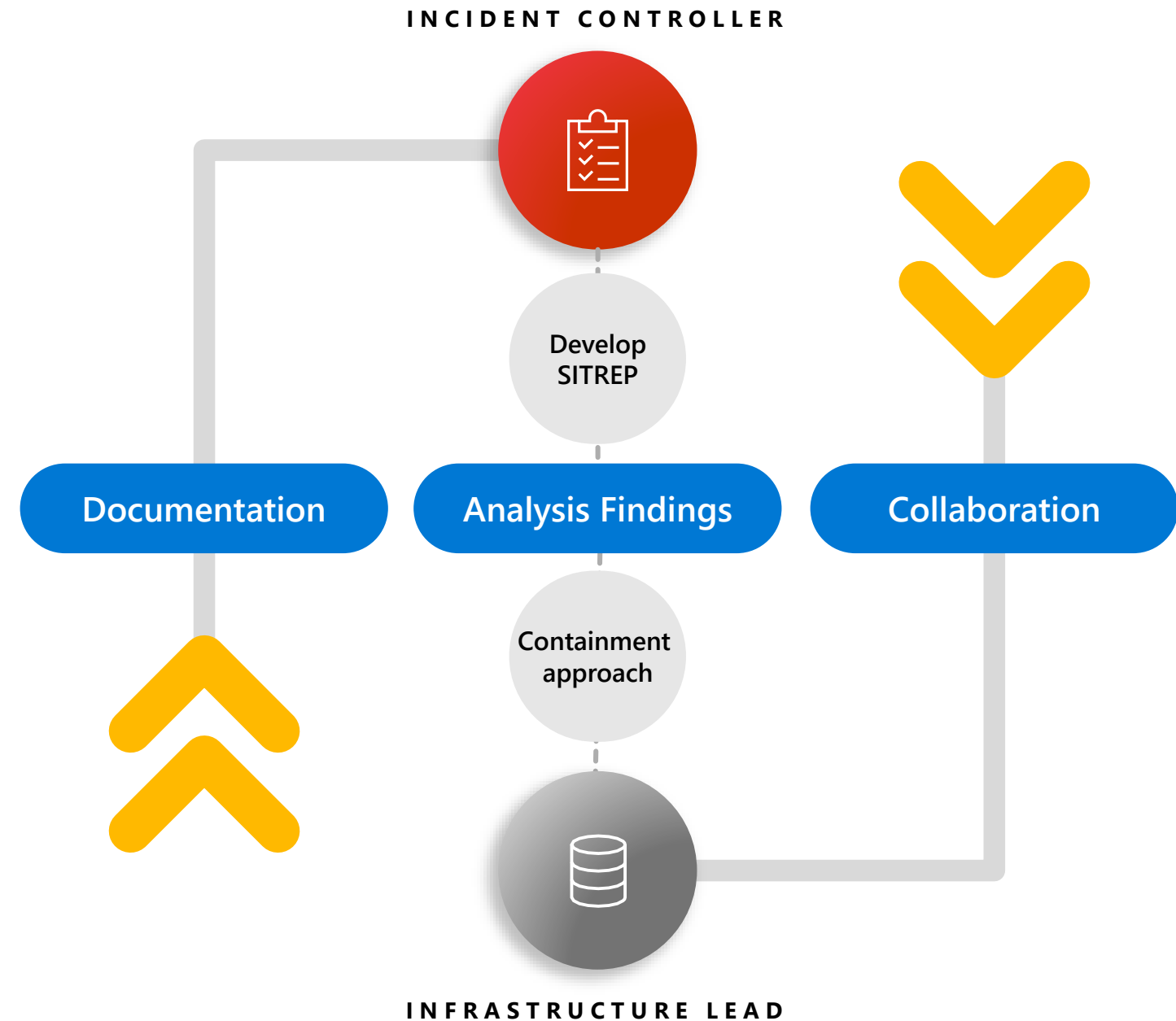
Clear documentation is a cornerstone of effective analysis; if it's not written down, it didn't happen.

It is imperative that key analysis findings are documented and shared with the wider response team so the impact of the findings is understood and can be translated to tasking for the other work streams, to manage and mitigate the risk.

Findings will inform an understanding of the risk for senior stakeholders, containment actions by the infrastructure workstream, details for both internal and external communications, and inform assessments for the regulatory workstream.

Collaborating roles:

[Incident Controller](#) → [Infrastructure Lead](#) →





Investigation Lead



Coordinate forensic investigation

Forensic investigations can be complex and may require support from multiple staff to efficiently assess the situation. The Investigation Lead must coordinate and prioritize forensic analysis tasking effectively.

Common pitfalls

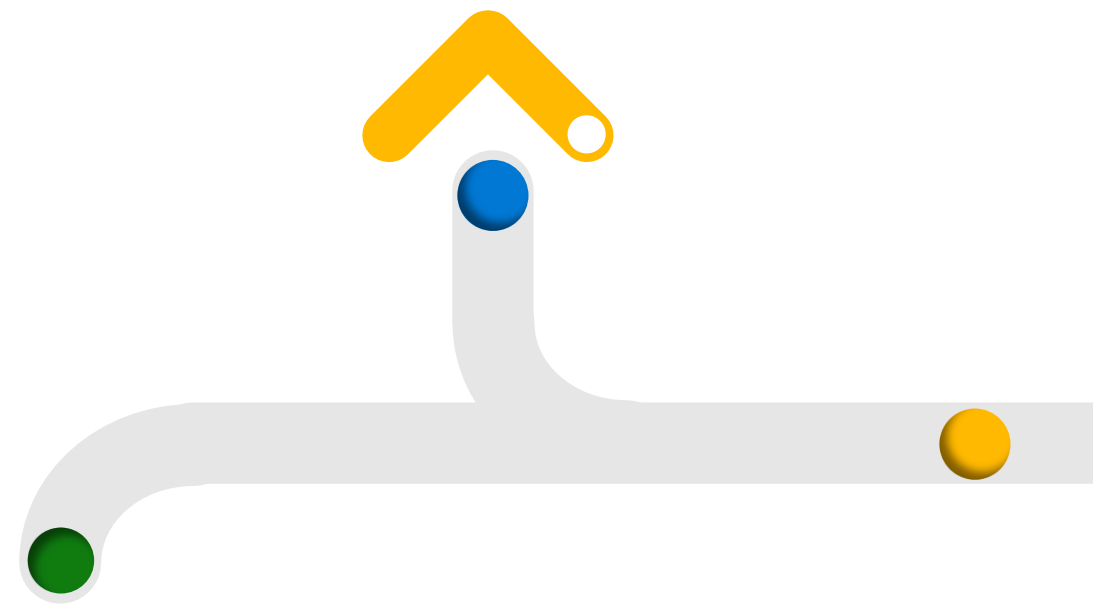
Analysts may gravitate towards more interesting analysis tasks, such as malware reverse engineering. While this may provide useful insights, it may be time consuming and other more pressing tasks could be addressed first. Ensure that tasks are prioritized based on risk.

Collaborating role:
[Infrastructure Lead](#) →

Analysis

The analysis process is iterative and will need to continue throughout the response. Findings will need to inform subsequent tasking, with the Investigation Lead ensuring that analysis goals are clear and that objectives are being met.

Analysis findings will inform other workstreams as the response progresses.





Investigation Lead



Proactive monitoring

Proactive monitoring of the network throughout the incident lifecycle goes hand in hand with the analysis of historical data to understand what occurred. This becomes crucial if the Threat Actor is still active in the environment.

Investigators should have the ability to create analytics to identify malicious activity, perform proactive hunting across the network where needed, and have the autonomy to take action on alerts of varying severity as they are raised.

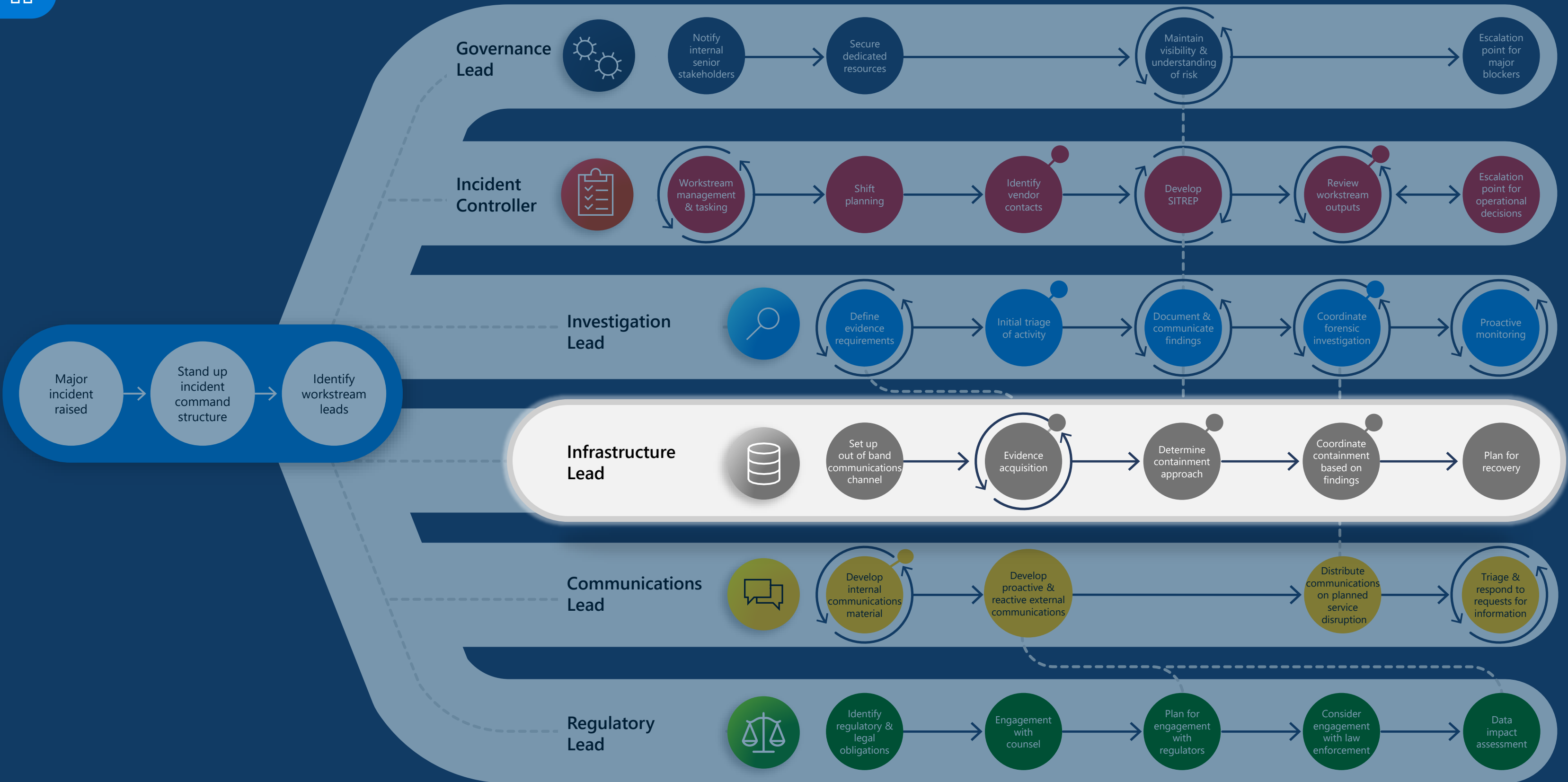
Common pitfall

Lack of proactive monitoring during an incident can lead to a resurgence of malicious activity going undetected. It is important that organizations have tooling in place that provides visibility of the environment of at ability to interdict should the threat actor attempt to re-establish a foothold in the environment.



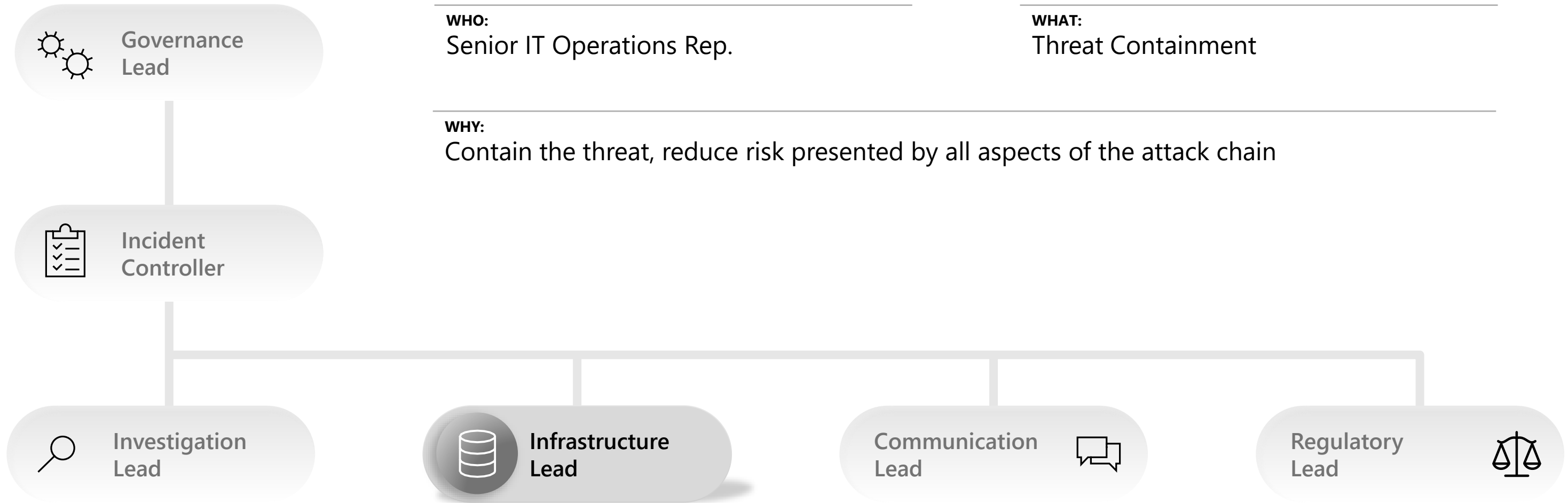
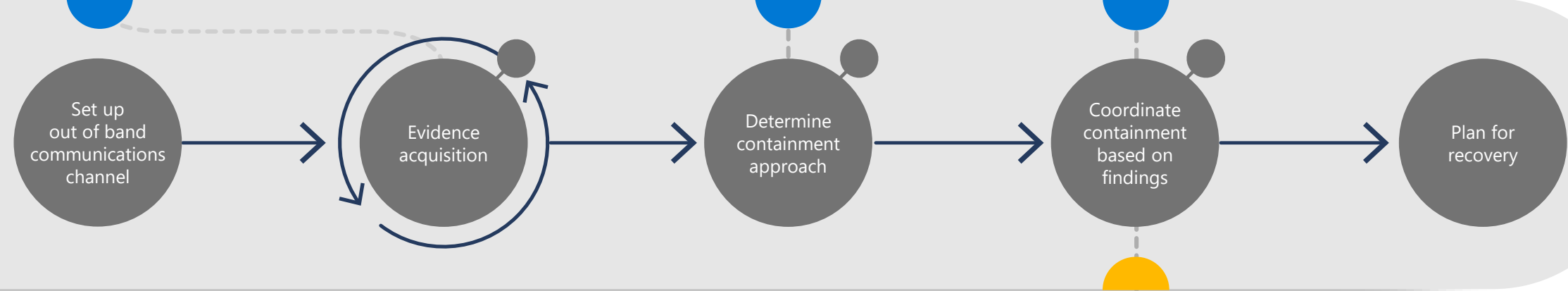
UP NEXT:

Infrastructure Lead



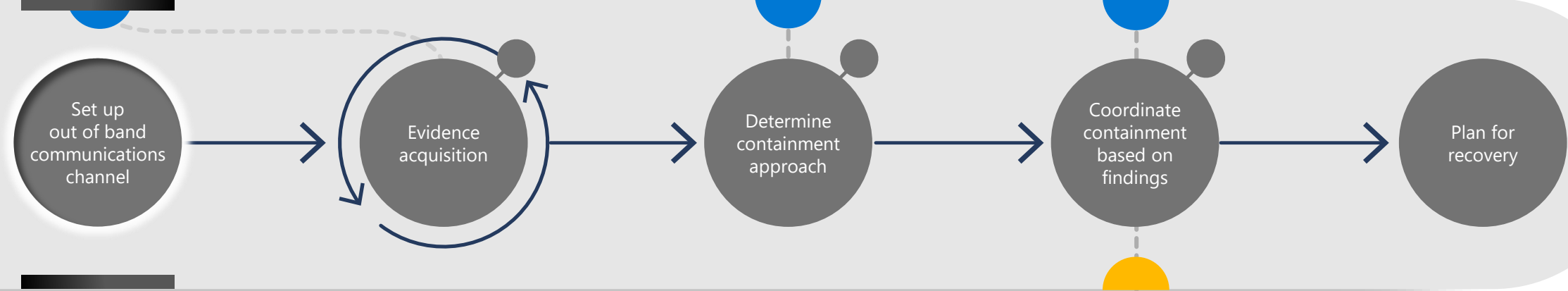


Infrastructure Lead





Infrastructure Lead



Set up out of band communications

At the outset of an incident, the true scope of the issue is hard to assess. Threat Actors may have a much deeper foothold in the environment than the initial detected activity suggests. As such, it is best to err on the side of caution and assume that communications may be intercepted.

Financially motivated and nation state actors have been known to monitor the communications of individuals involved with the response to understand containment and remediation activities, with a view of circumventing them. To mitigate this, organizations should consider using an out of band communications channel:



Move all communication related to the incident to a secure channel, ideally off the network which has been impacted.



This may require using standalone devices with a secure messaging application or email service that is not tied to the impacted network.



Consider limiting communications to individuals on a need-to-know basis. A vendor may need to know about a response to prioritize support requests, but may not require all the details



Leverage a codename for the incident response or a generic term when discussing the event, to avoid drawing unnecessary attention to the response.



Business units and application owners may need to be aware that there is response underway but may not require all the detail about the response and remedial activities.

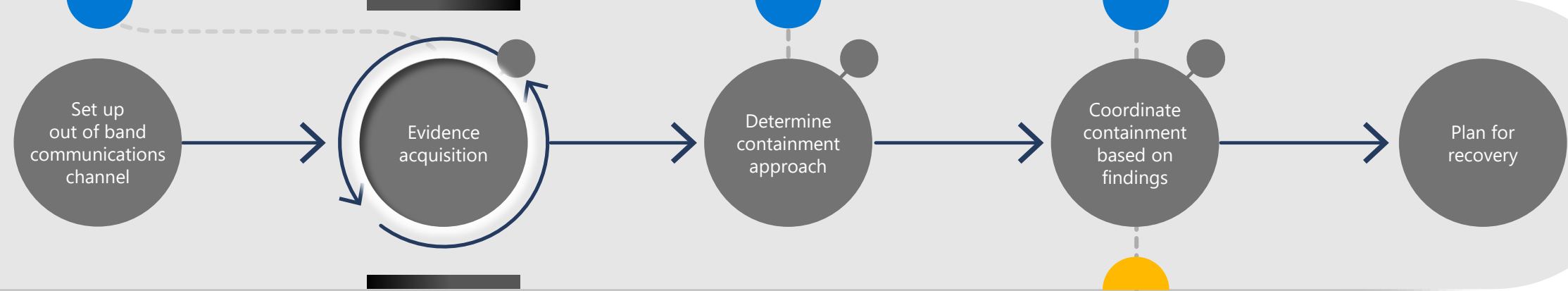
Collaborating role:
[Investigation Lead](#) →

Common pitfall

Organizations often skip this step, as moving to an out of band communications channel may be inconvenient. However, it is vital to ensure that communicates are kept private until you have confidence that your regular communication channels have not been compromised.



Infrastructure Lead



Evidence acquisition

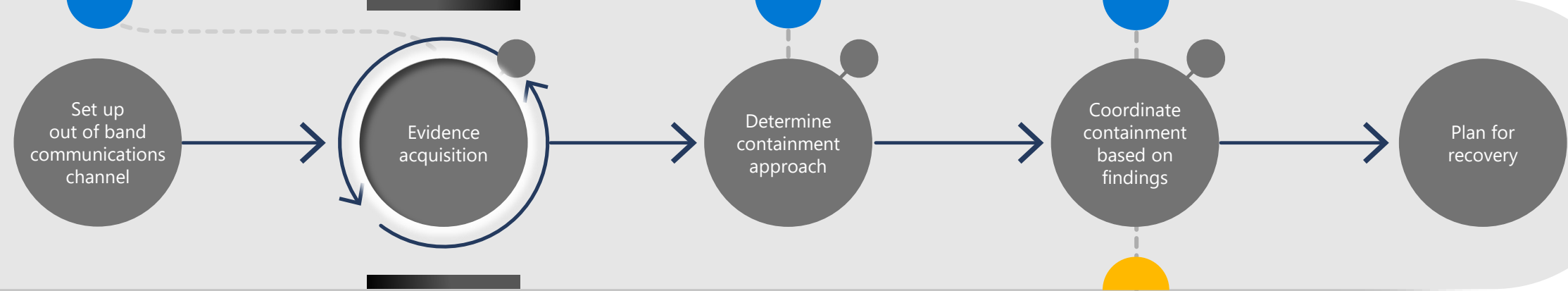
Timely evidence acquisition will enable the Investigation Lead to coordinate forensic analysis. In turn, this will allow for efficient containment as an understanding of the threat is developed. While the Investigation Lead will define evidence requirements, the Infrastructure Lead will facilitate evidence acquisition. In addition, the Infrastructure Lead will have valuable contextual knowledge around how the network is architected and what evidence may be available to support the investigation.



Collaborating role:
[Investigation Lead →](#)



Infrastructure Lead



Evidence acquisition

>> Historical Data

>> Live Data

>> Contextual Data

On-Premises



EVIDENCE TYPE: Historical Data

✓ Triage Images

Collection can be performed using several open-source tools which can be deployed widely across the environment.

This allows for automated collection at scale, enabling efficient analysis.

✓ Disk Images

Collection will vary depending on the host, virtual machine snapshots, or virtual disks can be leveraged, whereas physical hosts will require images to be created using a collection tool.

Consider creating a physical image as opposed to a logical image to enable file carving and recovery.

May be required where connectivity across the network is limited due to containment.

✓ Memory Images

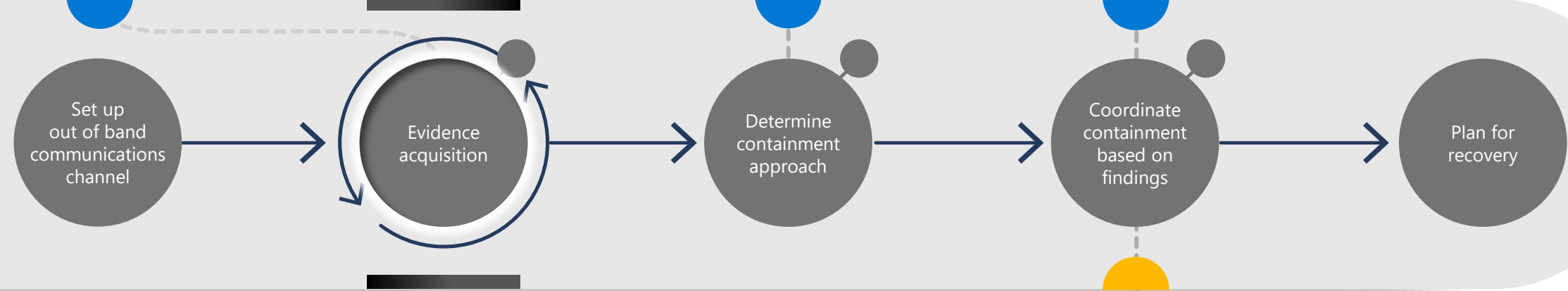
Requires a memory acquisition tool to be run on a live host.

Memory collection may have limited utility on a host that was powered off during containment or recently restarted.

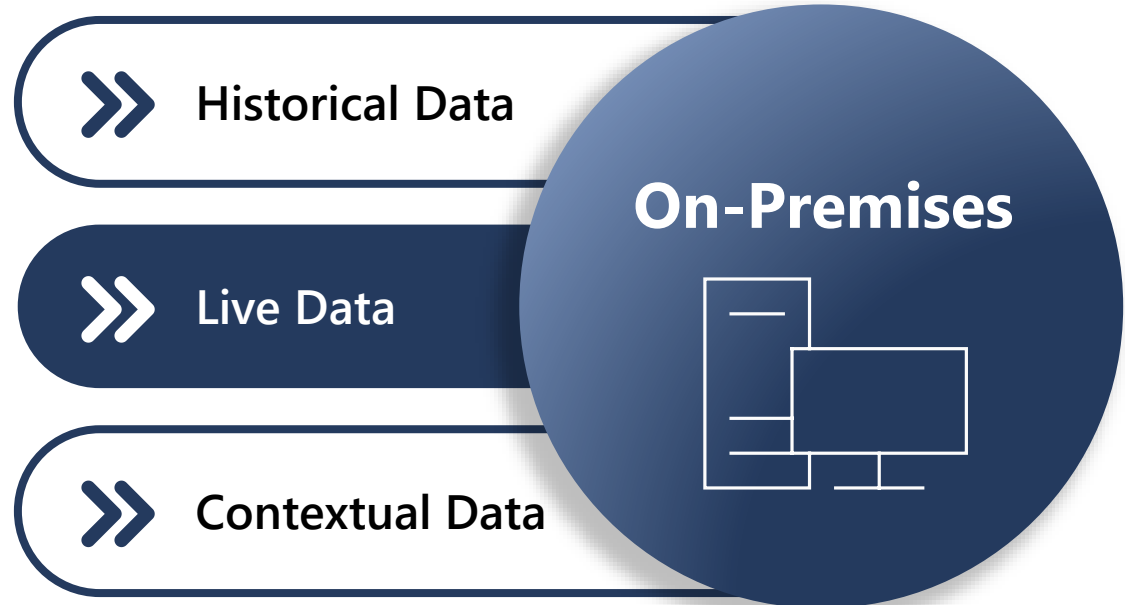
Collaborating role:
[Investigation Lead](#) →



Infrastructure Lead



Evidence acquisition



EVIDENCE TYPE: Live Data

✓ EDR Monitoring

EDR tooling should be deployed as widely as possible in the environment, with priority given to critical servers.
This will enable containment and active threat mitigation.

✓ Active Blocking or Auditing

Blocking mode is recommended regardless of the incident, along with a robust process to triage and deconflict block events as they occur.
Note that having multiple EDR solutions deployed to the same host may cause functionality issues.

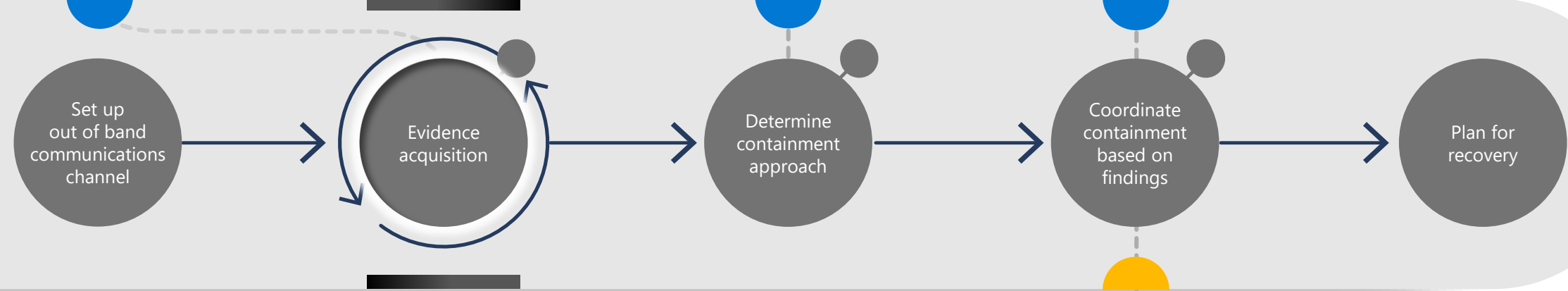
✓ Custom Alerting

During deployment, knowledge transfer with the Investigation Lead around using the product effectively to create custom indicators and detections should be prioritized.

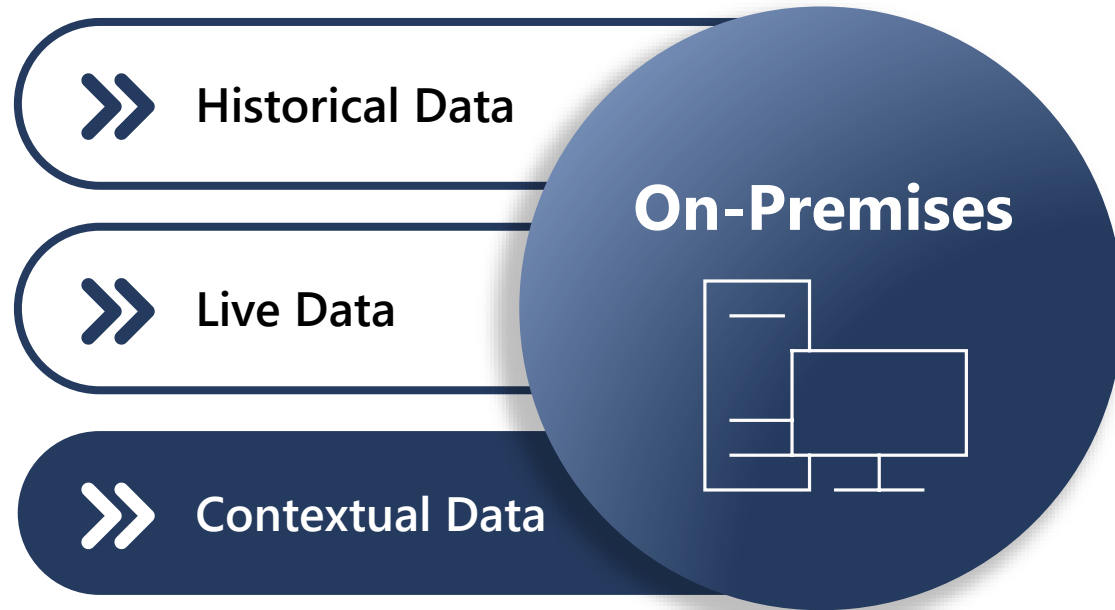
Collaborating role:
[Investigation Lead](#) →



Infrastructure Lead



Evidence acquisition



Collaborating role:
[Investigation Lead](#) →

EVIDENCE TYPE:
Contextual Data

- ✓ **Boundary Device Logging**

Logging from key devices such as firewalls, VPN appliances, proxies, and internet exposed web servers should be collected.

Ensure understanding of what data is being logged and log retention time frames.

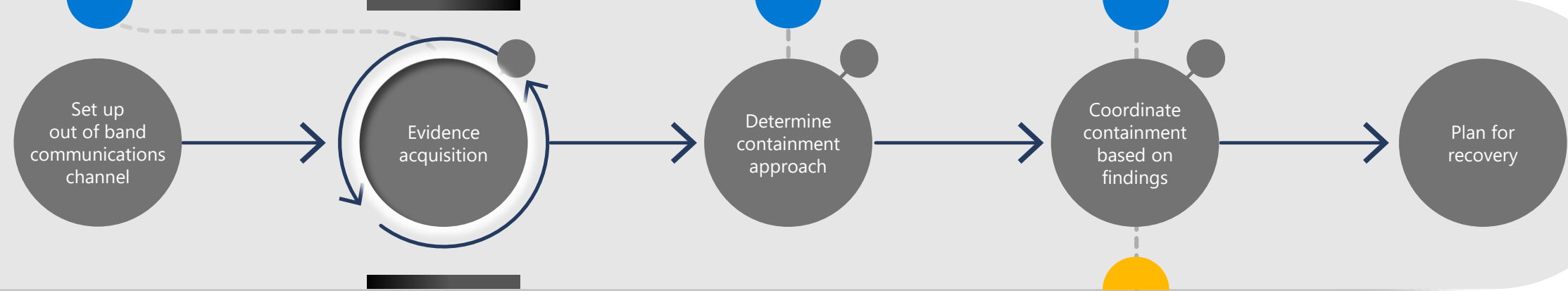
Appropriate configuration of this logging is key to ensure it has utility during an investigation.
- ✓ **Centralized SIEM**

Ensure analysts are provided with access to the SIEM solution and understand what data is captured.
- ✓ **Remote Access Architecture**

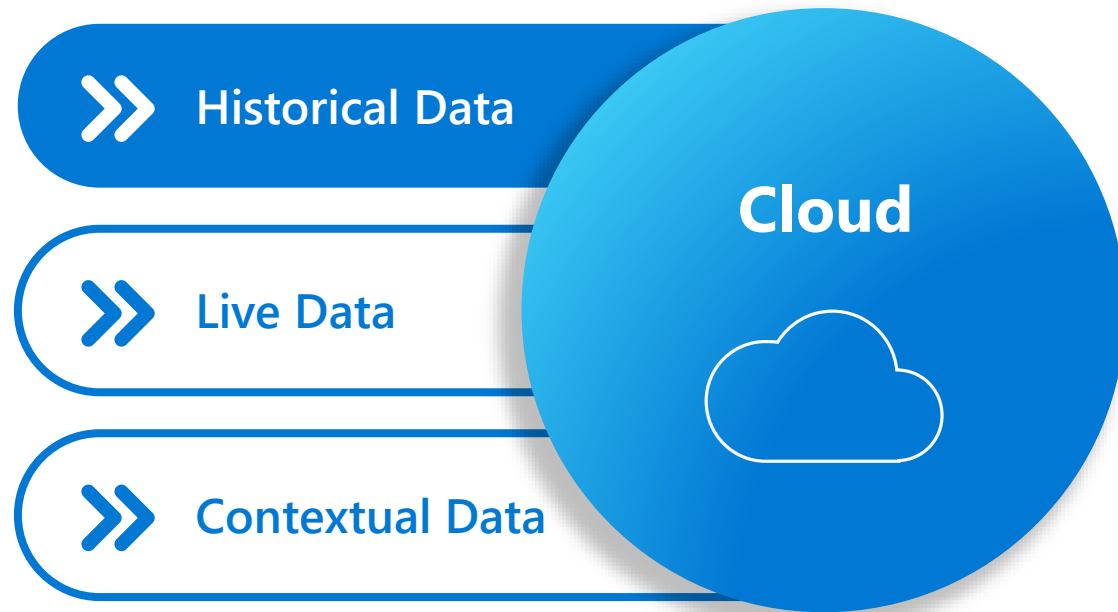
Effective communication between the Investigation Lead and Infrastructure Lead is crucial to developing an understanding of remote access methods and authentication flows.



Infrastructure Lead



Evidence acquisition



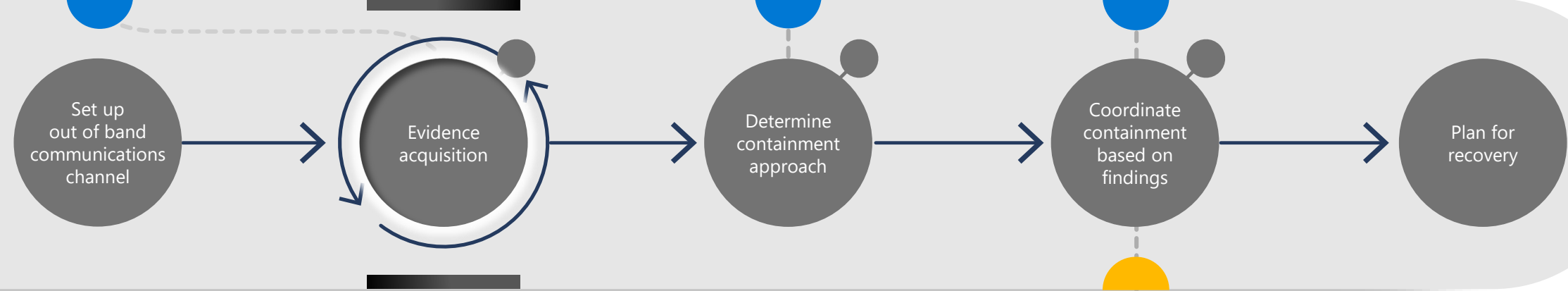
Collaborating role:
[Investigation Lead](#) →

EVIDENCE TYPE: Historical Data

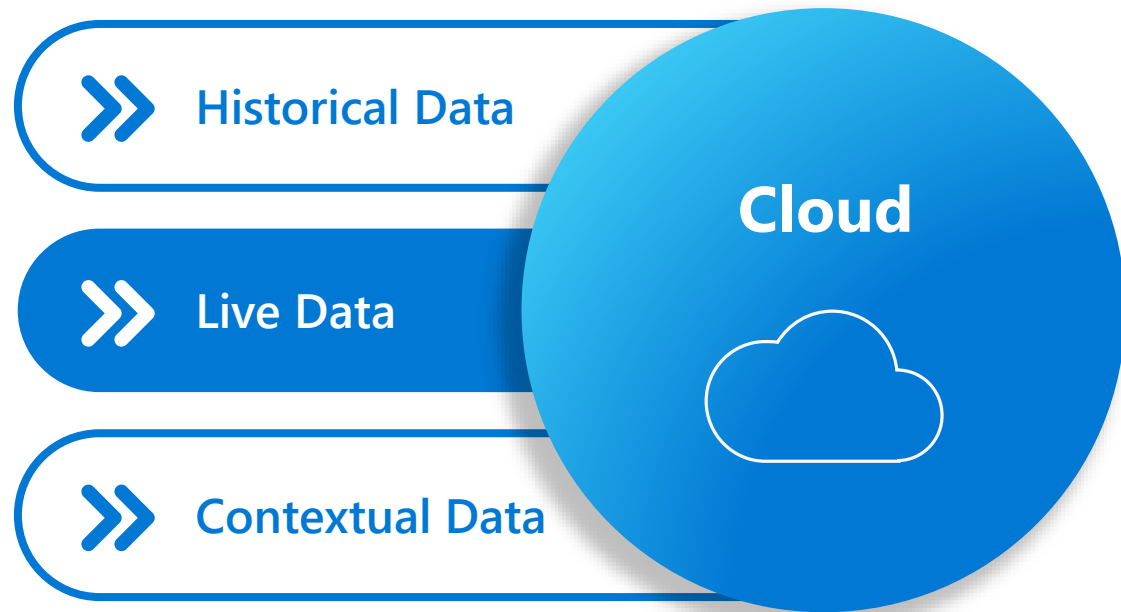
- ✓ Sign-in & Audit Logging**
 If not centralized, this logging is only available for the past 30 days in Microsoft security portals (may vary for other cloud platforms).
 Ensuring this data is exported at the outset of an incident to ensure all possible evidence is available to analysts.
- ✓ Application & Activity Logging**
 If not centralized, this logging is only available for the past 30 days in Microsoft security portals (may vary for other cloud platforms).
 Ensuring this data is exported at the outset of an incident to ensure all possible evidence is available to analysts.
- ✓ Cloud Resource Artifacts**
 Once a resource is deleted there it may not be recoverable, meaning that key evidence may be unavailable; ensure robust processes are put in place to isolate and maintain resources of interest until analysis is complete.



Infrastructure Lead



Evidence acquisition



EVIDENCE TYPE:

Live Data

✓ Identity & Email Provider Alerting

If not already in place, ensure each of these alerting streams are configured and enabled at the outset of an incident, with a robust alert triage process established; false positives will be present so deconfliction and tuning may be required.

✓ Custom Alerting: Sign-in Events

As the investigation begins and compromised identities are found, ensure alerting is put in place to monitor any activity from those identities. Consider leveraging honey tokens to support this.

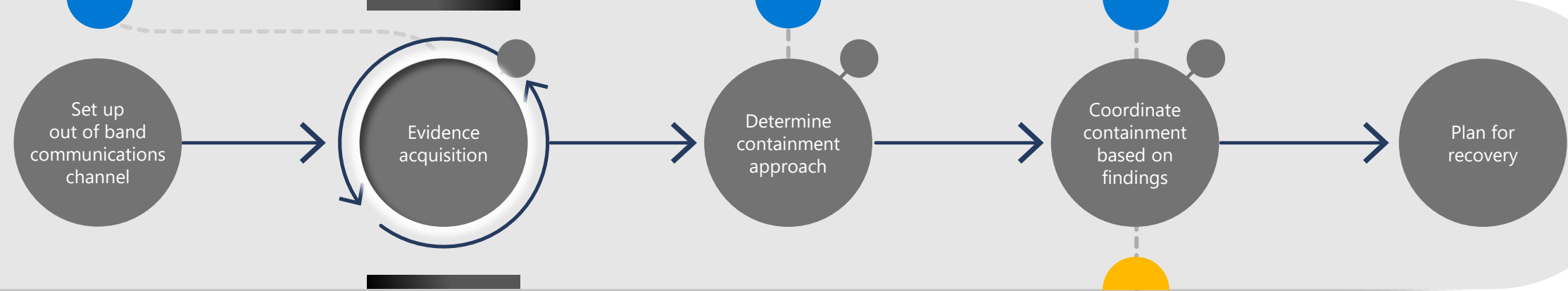
✓ Custom Alerting: Admin Audit Logs

All activities undertaken by a Threat Actor should continue to be monitored closely; if a TTP worked once the odds of it working again are high and are the path of least resistance for any active Threat Actor.

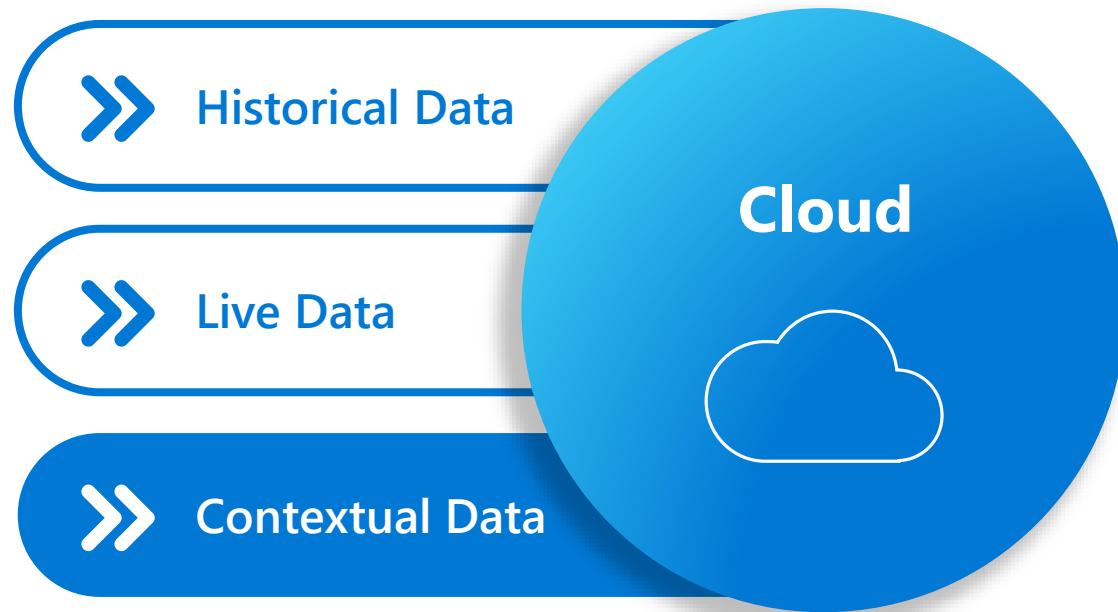
Collaborating role:
[Investigation Lead](#) →



Infrastructure Lead



Define evidence requirements



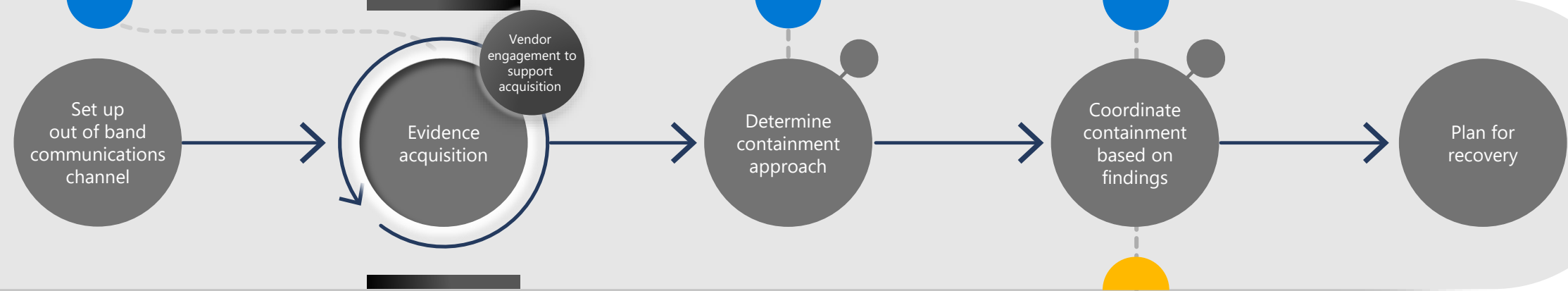
EVIDENCE TYPE: Contextual Data

- Auth & Email Flow Architecture**
 Effective communication between the Investigation Lead and Infrastructure Lead is crucial to developing an understanding of authentication and email flows.
- Centralized SIEM**
 Ensure all analysts are provided with access to this tool and knowledge transfer on the data contained within is prioritized.
- Hybrid Architecture**
 Effective communication between the Investigation Lead and Infrastructure Lead is crucial in developing an understanding of on-premises and cloud topology.

Collaborating role:
[Investigation Lead](#) →



Infrastructure Lead



Evidence acquisition

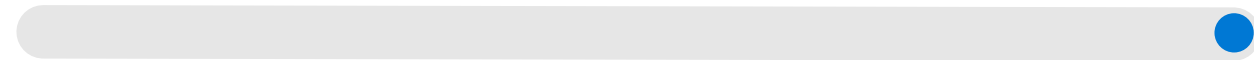
Vendor engagement to support acquisition

An organization may rely on multiple vendors for specific IT services or may outsource the entirety of their IT operations. Evidence acquisition may require the support of vendors who manage platforms and services on behalf of the organization.

Evidence acquisition may require tooling to be run on an impacted host. Staff performing acquisition may not be familiar with these tools. Clear guidance should be given on what evidence items are required and how the evidence is to be collected, so data is acquired as quickly as possible to support the investigation.

Common pitfall

If proactive engagement with vendors has not occurred, they may not prioritize requests for evidence acquisition. These sorts of request are atypical and require vendors to run tools they may be unfamiliar with. If clear guidance is not provided, incomplete or irrelevant evidence may be collected.



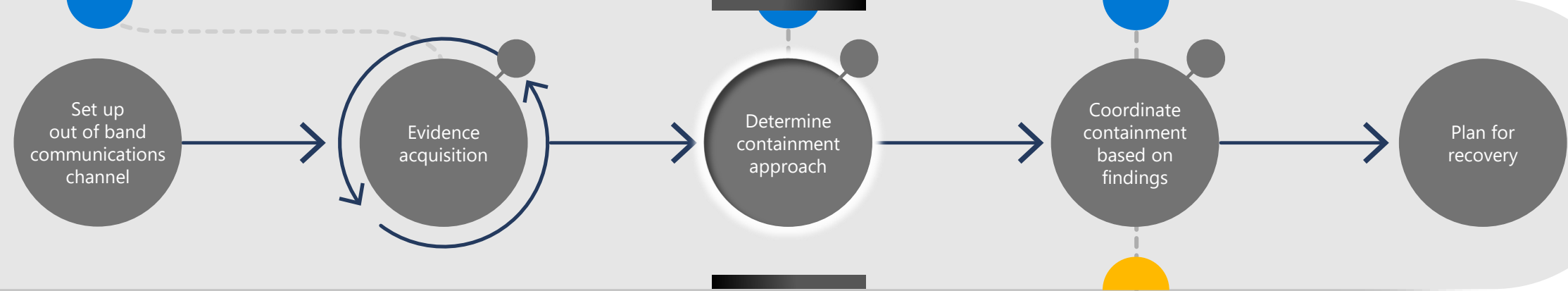
Consider a scenario where a virtual mail server has been compromised and a disk image is required for analysis. Clear guidance has not been provided to the vendor, which results in a snapshot of the VM from before the compromise being provided for analysis. In addition, the OS disk and the disk housing the mail data are provided. The disk containing the mail data is significant in size, delaying the copy and transfer of the data, ultimately slowing progress on the investigation.



Collaborating role:
[Investigation Lead →](#)



Infrastructure Lead



Determine containment approach

Containment activities tactically limit the Threat Actor’s ability to traverse the environment and achieve their actions on objective. When carrying out containment, a balance needs to be struck between hindering the actor and causing business disruption as a result of implementing containment measures. In addition, consideration needs to be given to how the containment measures may alert the actor to the response.

The containment approach should be based on the type of incident. In general, if there is evidence the actor intends to take destructive action or is financially motivated, containment should be prioritized at the expense of business impact and alerting the Threat Actor.

If, however, the intrusion is historic and look to be carried out by an espionage-motivated Threat Actor, consider that they may have multiple points of presence in the environment and could be well entrenched. Performing containment prematurely—before proper scoping and investigation have been performed—may alert the actor to the response. As a result, they may cease interacting with the network to avoid detection, or proactively remove some of their persistence mechanisms.

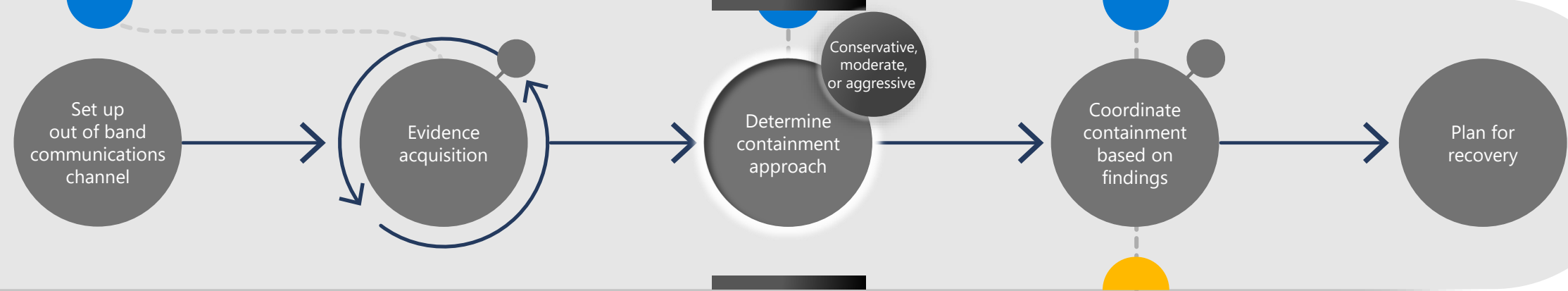


In summary, make risk-based, evidence-informed decisions on when to begin containment to ensure you adequately contain the threat.

Collaborating role:
[Investigation Lead →](#)



Infrastructure Lead



Determine containment approach

Conservative, moderate, or aggressive

INCIDENT TYPE

Historical Compromise

Dwell time in the network is extended, activity identified likely motivated by data collection, and exfiltration

Detected Compromise

Actor detected before completing actions on objectives, motivation not clear, more information needed

Destructive Compromise

Actor takes overt actions swiftly with a clear motivation to establish dominance and employ destructive strategies

CONTAINMENT STEPS

Conservative

Prioritize scoping and investigation of compromise before containment

Undertake containment following the investigation, default action to monitor

Strong consideration should be given to impact of containment actions on business operations

Moderate

Prioritize containment of persistence mechanisms, impacted identities, and devices

Undertake containment actions based on continuous risk assessment, default action to block

Moderate consideration should be given to impact of containment actions on business operations

Aggressive

Prioritize containment of tier-0 assets, identities, and remote access solutions

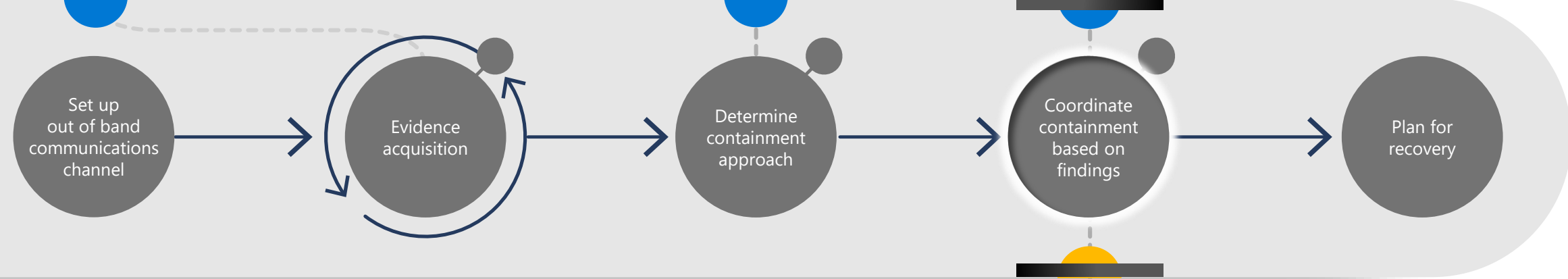
Undertake containment actions in near real time, default action to block

Limited consideration for impact of containment actions on business operations

Collaborating role: [Investigation Lead](#) →

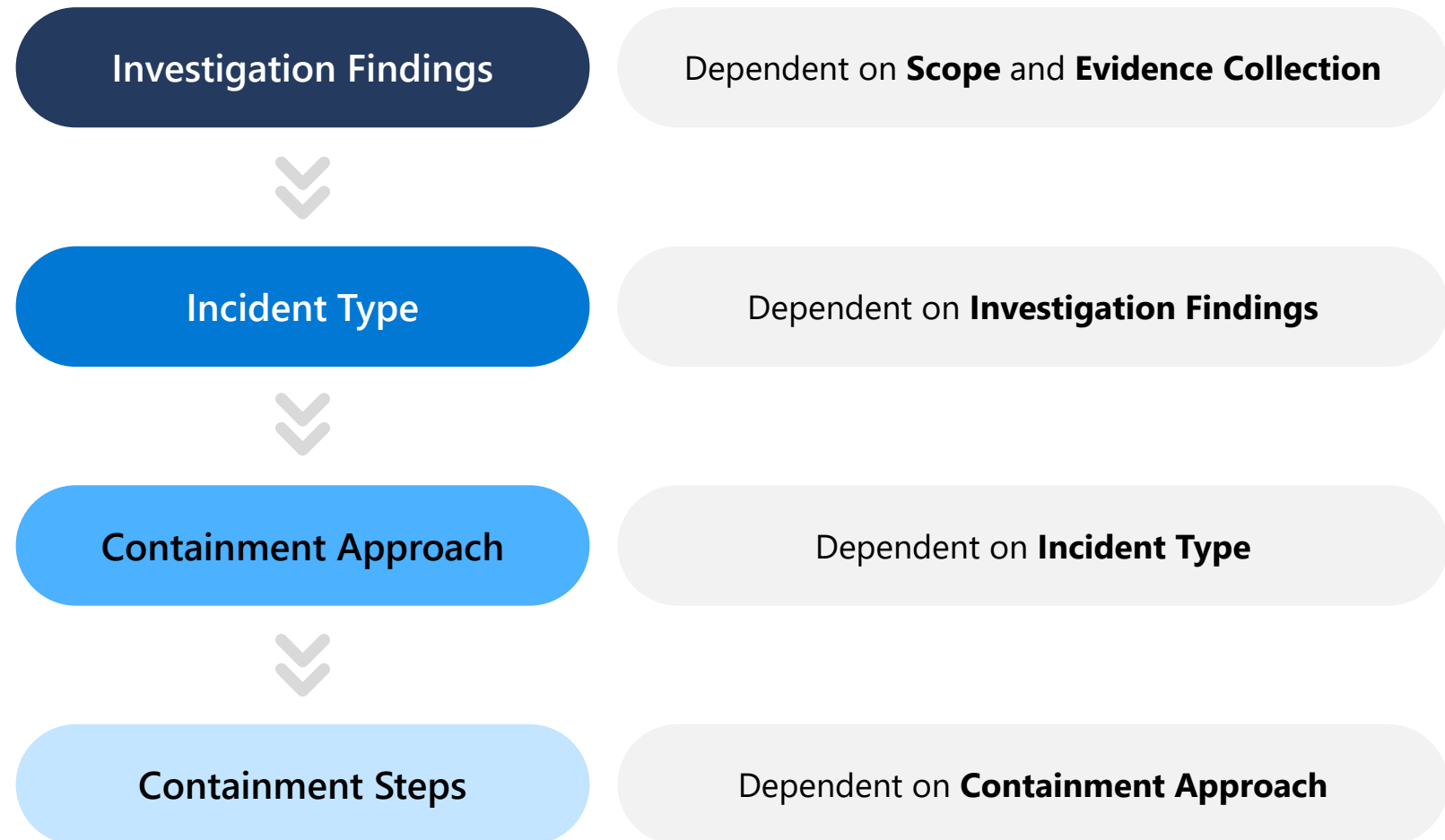


Infrastructure Lead



Coordinate containment based on findings

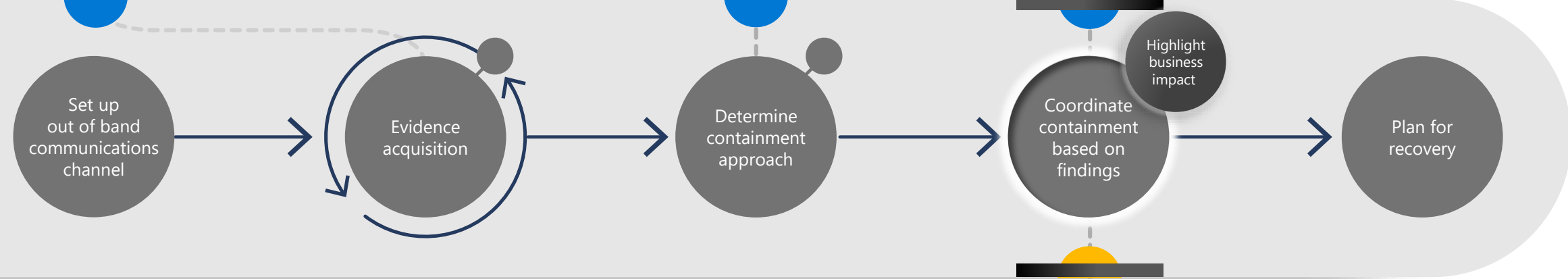
The specific containment actions taken should be evidence driven to balance mitigation of risk and disruption to service. Action should align with the containment approach: conservative, moderate, or aggressive.



Collaborating role:
[Investigation Lead](#) → [Communications Lead](#) →



Infrastructure Lead

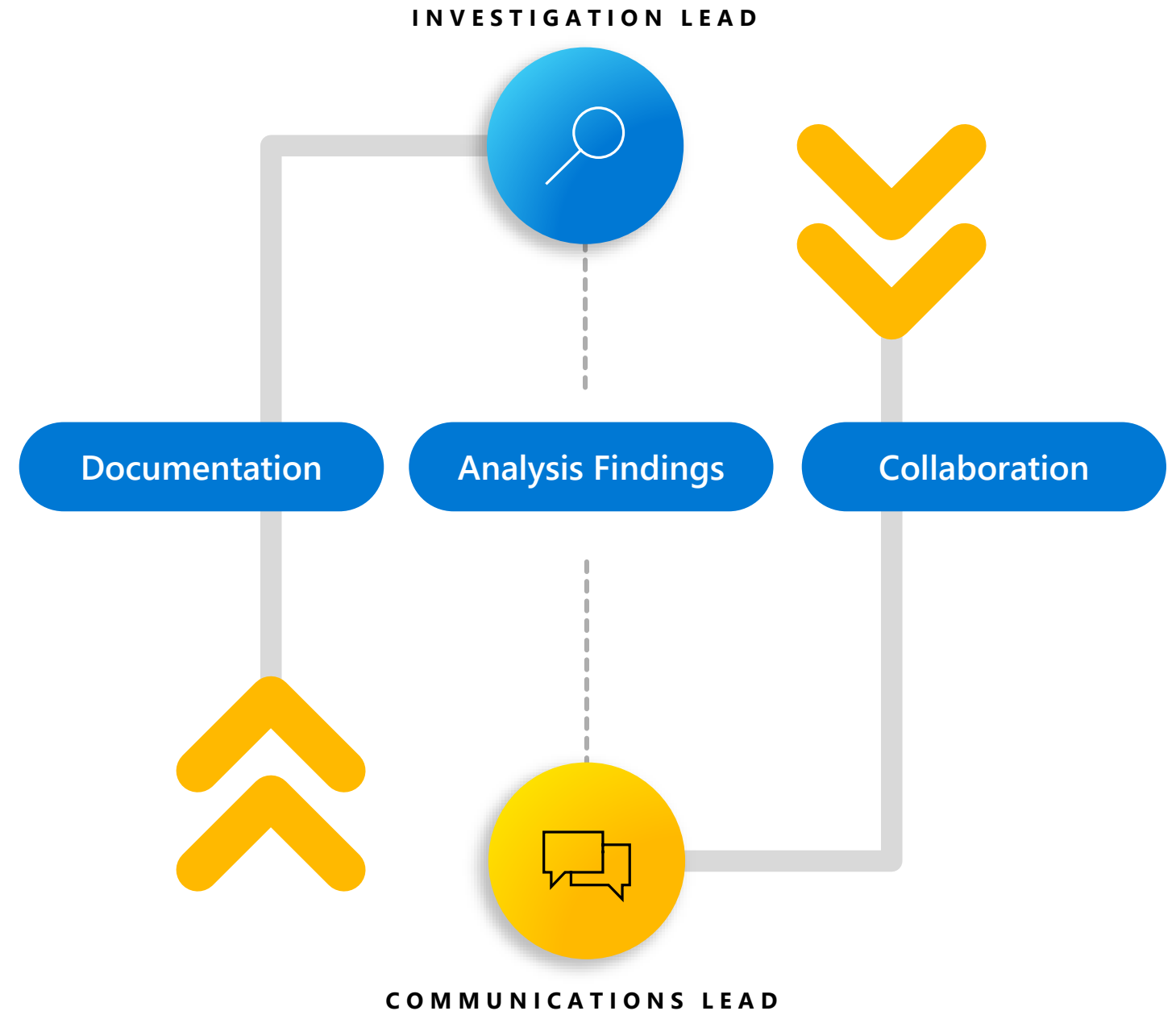


Highlight business impact

Response activity may cause business disruption. For example, if a host running a business-critical application needs to be contained. While the response team should have the autonomy to take actions that limit the Threat Actor's ability to traverse the network, consideration should still be given to how this will affect services.

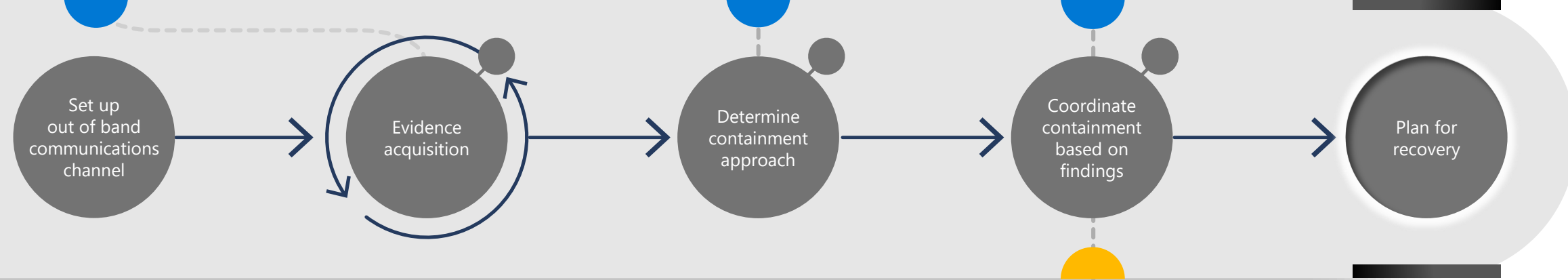
The Infrastructure Lead should have a clear picture of the impact that containment actions will have on the business and should relay this to the Communications Lead. The Communications Lead can then make the business aware of service disruption and manage any questions or concerns from other stakeholders, with support from the Incident Controller and Governance Lead if required.

Collaborating role:
[Investigation Lead](#) → [Communications Lead](#) →





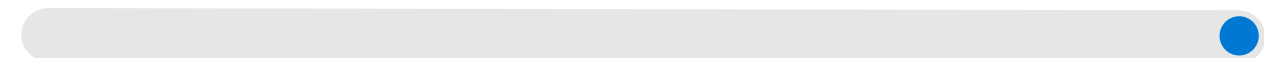
Infrastructure Lead



Plan for recovery

While containment stems the bleeding and addresses the immediate risk, recovery will address longer term return to service work items and hardening.

Through response activities, an understanding of the risk and where the potential gaps in an organization's security aperture will be developed. Recovery work items should be framed around addressing those risks in order of priority.



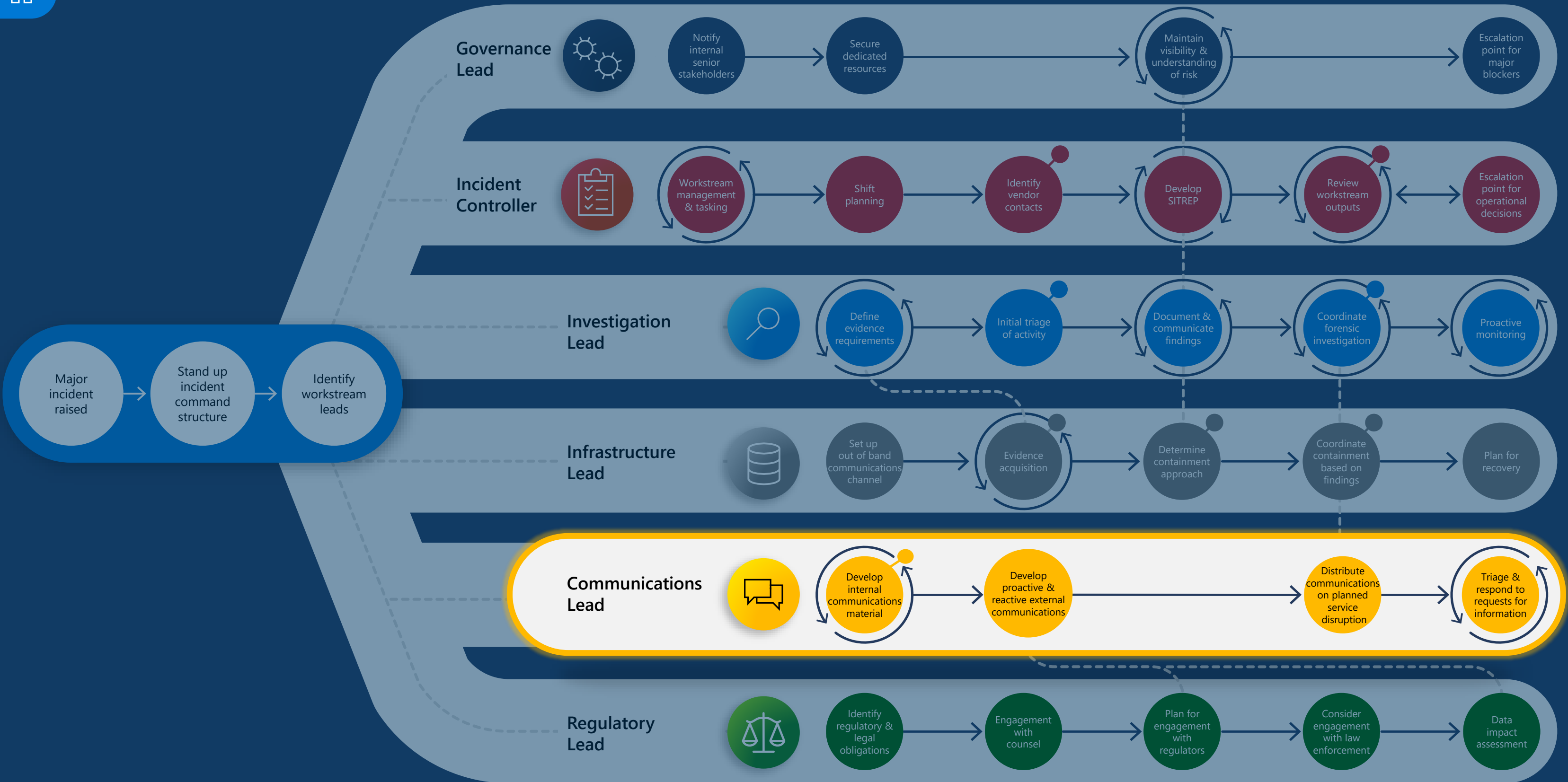
Additional Resources

- [Cybersecurity Recovery & Remediation After a Security Breach](#)
- [Microsoft security incident management: Post-incident activity - Microsoft Service Assurance | Microsoft Learn](#)



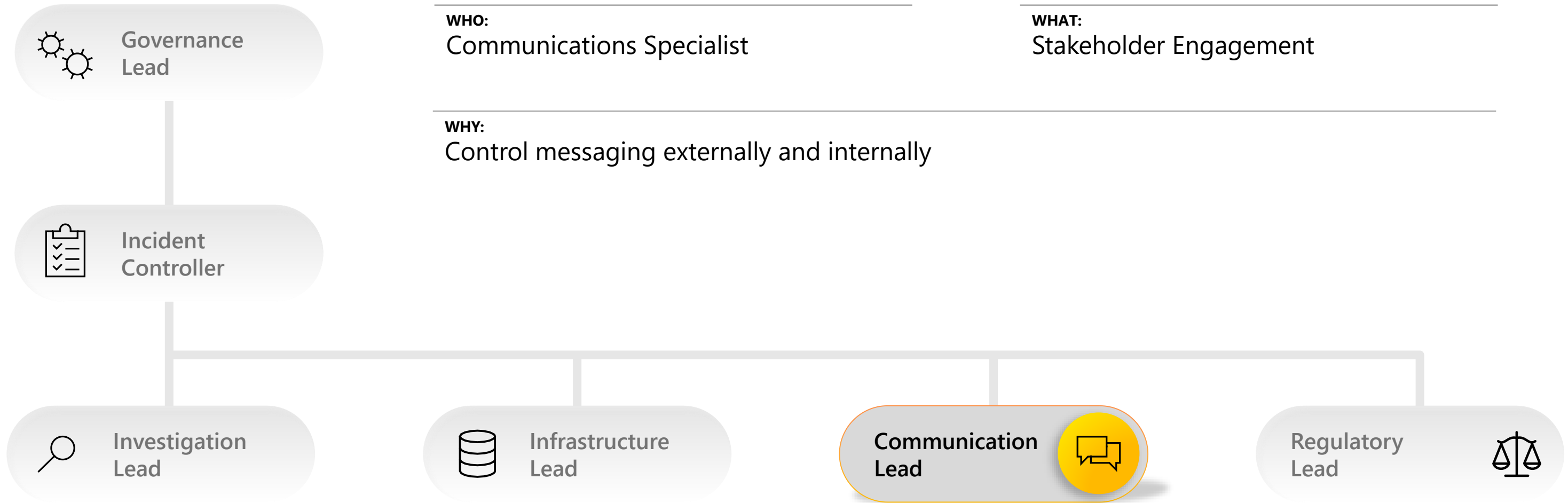
UP NEXT:

Communications Lead





Communications Lead



Governance Lead

WHO:
Communications Specialist

WHAT:
Stakeholder Engagement

WHY:
Control messaging externally and internally



Incident Controller



Investigation Lead



Infrastructure Lead

Communication Lead

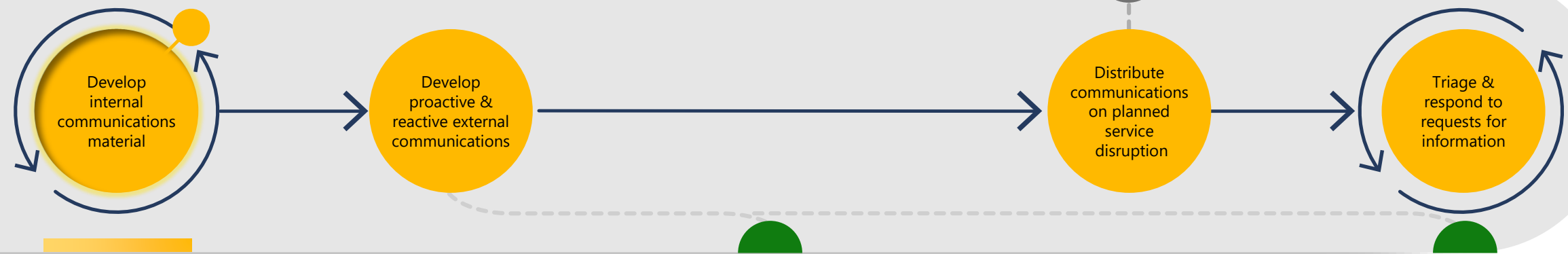


Regulatory Lead





Communications Lead



Develop internal communications material

While SITREPs should be used to maintain a single source of truth on the status of the incident and action tracking for those directly involved, there may still be a need for wider communication internally. The intent of these communications is to proactively notify key stakeholders of potential business disruption, either as a result of Threat Actor activity or as part of containment. When developing these communications, implement the “need to know” principle—only provide information which is relevant to stakeholders as opposed to details about the investigation or specific actions taken by the threat actor.

- ✓ A high-level statement either communicating that an incident is being managed, or a generic statement about an IT issue which is being addressed
- ✓ If an incident is disclosed, include high level information on what is being done to address the threat.

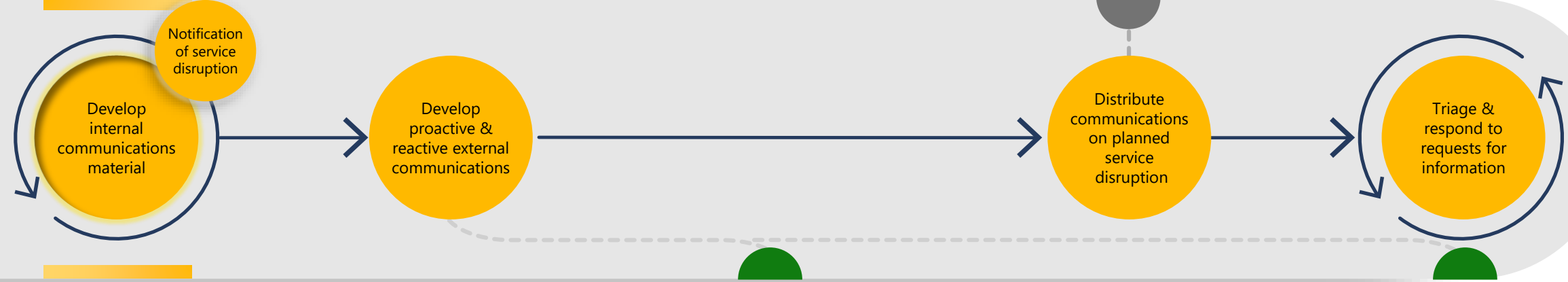
- ✓ Information about current service disruption with an expected timeframe for service restoration, if known
- ✓ Information about planned service disruption as a result of containment activities with an expected timeframe for service restoration, if known

- ✓ Clear guidance on what can and can't be communicated to other staff internally
- ✓ Clear guidance on what can and can't be communicated to customers or other external parties, in accordance with an external communication plan

- ✓ Contact details for the Communications Lead or a delegate, should recipients have questions or concerns
- ✓ An indication of when the next update can be expected



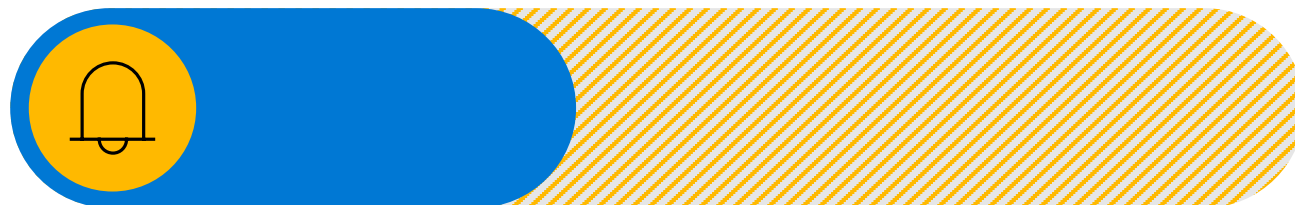
Communications Lead



Develop internal communications material

Notification of service disruption

If an incident has caused an outage or service disruption, this may be visible across the organization. Where possible, the Communications Lead should control messaging and proactively notify stakeholders of the issue, in line with the internal communications material.



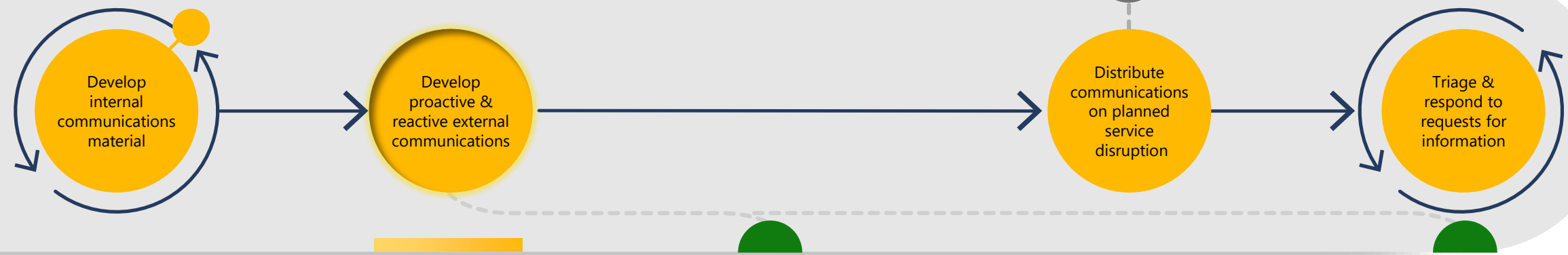
Common pitfall

These wider communications may need to be delivered over the compromised network. As such, their content should be scrutinized to ensure that they do not provide information which the threat actor could leverage to circumvent the investigation and containment activity.

Plan for this communication to be leaked or disclosed publicly. To mitigate the risk, limit dissemination and ensure the content is in line with external communications being developed.



Communications Lead



Develop proactive and reactive external communications

During an incident, organizations place emphasis on limiting external communications to minimize reputational damage. At times, the service disruption caused by an incident, or through containment actions, necessitates external communication.

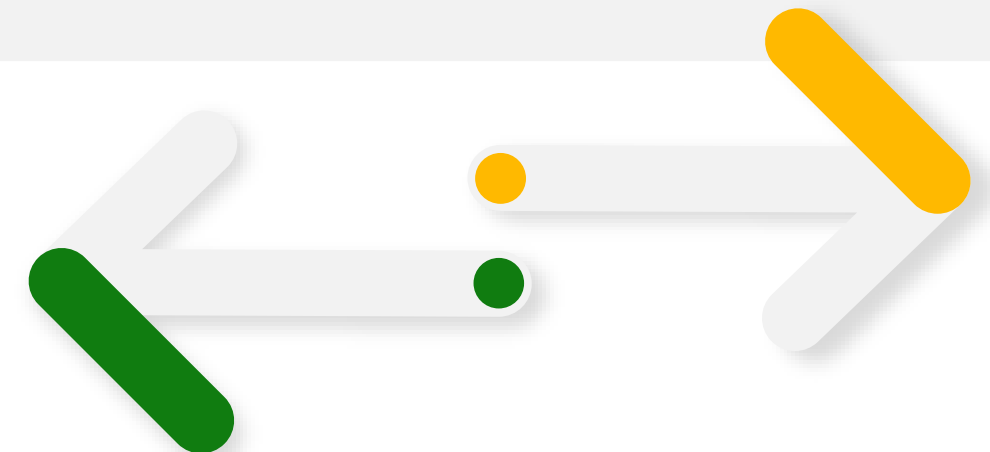
In the absence of direct communication, customers and partners will fill the information void with speculation about what has transpired and the risk this may pose to their own networks and data assets. To mitigate this, proactive and reactive communications should be developed to help control messaging and to provide reassurance to external parties that the right steps are being taken to address the issue.

The “need to know” principal should still be employed when developing these communications. There is a greater risk this information will be disclosed publicly as it is difficult to control dissemination of the communications material once it is shared.

Collaborating role:
[Regulatory Lead →](#)

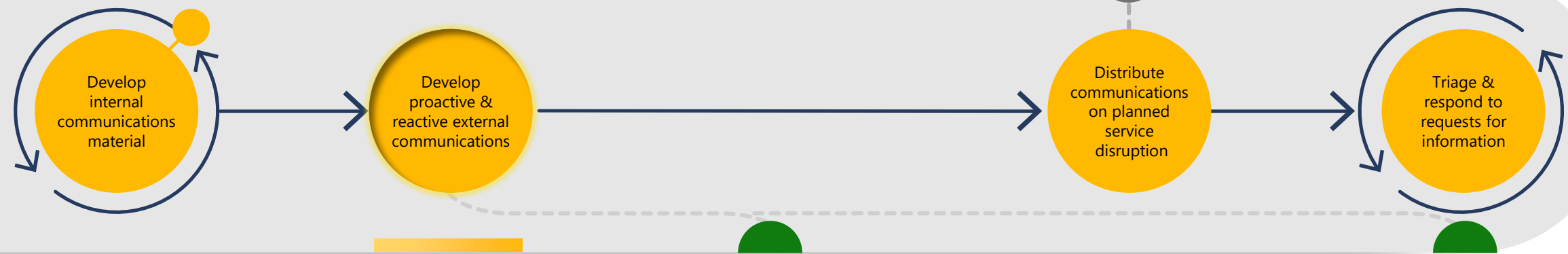
Common pitfall

When developing these communications, do not include authoritative statements which you may need to retract as the investigation progresses. For example, avoid stating that no customer data was impacted or exfiltrated before the investigation is complete. Instead, state that the investigation is ongoing, but to date has not identified evidence of impact to information assets.





Communications Lead



Develop proactive and reactive external communications

External communications may include:



A high-level statement either communicating that an incident is being managed or a generic statement about an IT issue which is being addressed



If an incident is disclosed, share high-level information on the actions being taken to address the issue, to provide assurance that the situation is being managed effectively.



If an incident is disclosed and the investigation has found impact to data assets, include high level information on impact to information assets or risk to your customers and partners.



Information about current service disruption with an expected timeframe for service restoration, if known

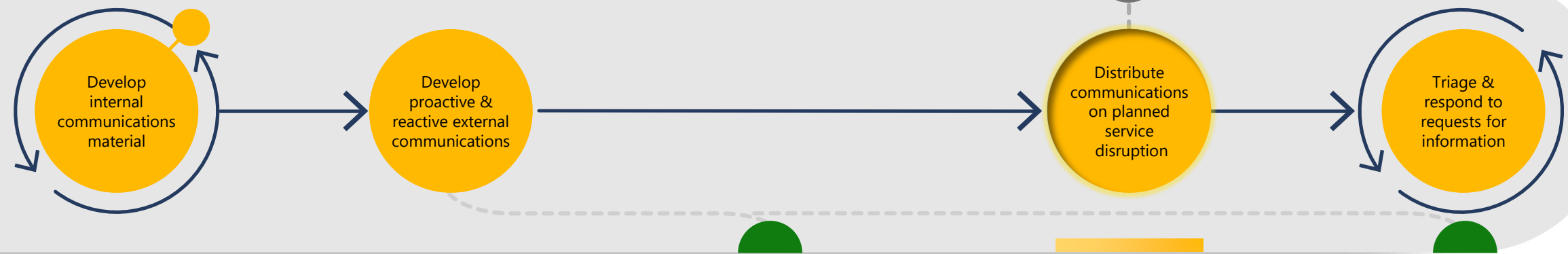


An indication of when the next update can be expected

Collaborating role:
[Regulatory Lead →](#)



Communications Lead

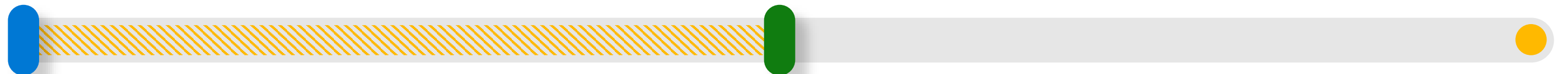


Distribute communications on planned service disruption

As containment actions are taken, there may be disruption to service as hosts are isolated and identities disabled. The Infrastructure Lead must develop an understanding of the business impact containment actions may have. This can be relayed to the Communications Lead to highlight to the business. Note that the response team should have the autonomy to take decisive action to contain the Threat Actor. Notification of service disruption should not take precedence over actual containment actions. Where possible, containment actions that cause impact should be followed by prompt communication—and if possible—a timeframe for when service will be restored.

Common pitfall

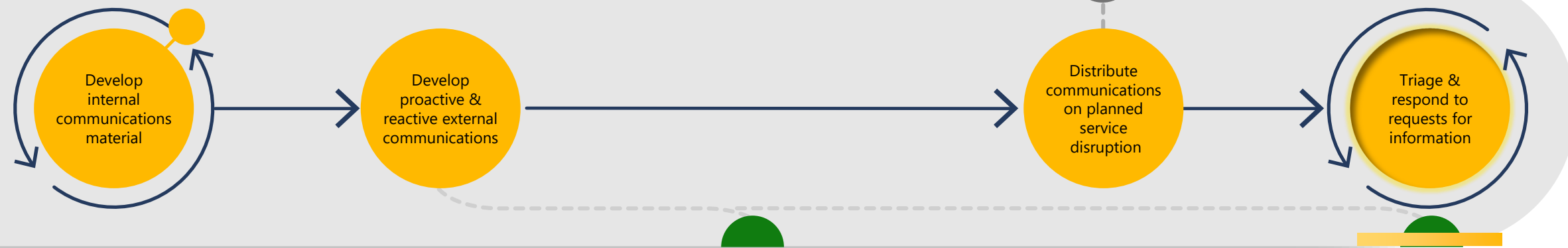
In the absence of this communication, internal and external parties may assume the worst as containment actions impact services. Timely communication on planned service disruption will help to control messaging and allay concerns as the response progresses.



Collaborating role:
[Infrastructure Lead →](#)



Communications Lead



Triage and respond to requests for information

Once communication on the incident has been distributed both internally and externally, expect that questions will be raised by a range of stakeholders. These requests may be from concerned internal stakeholders who hold relationships with customers or from customers themselves who want to understand the potential risk and impact to their data assets. Responses to these queries should be timely to maintain trust but should be in line with either the internal or external communications material developed. While answers to all the possible questions may not be available, a balance needs to be struck between transparency and maintaining the integrity of the investigation.

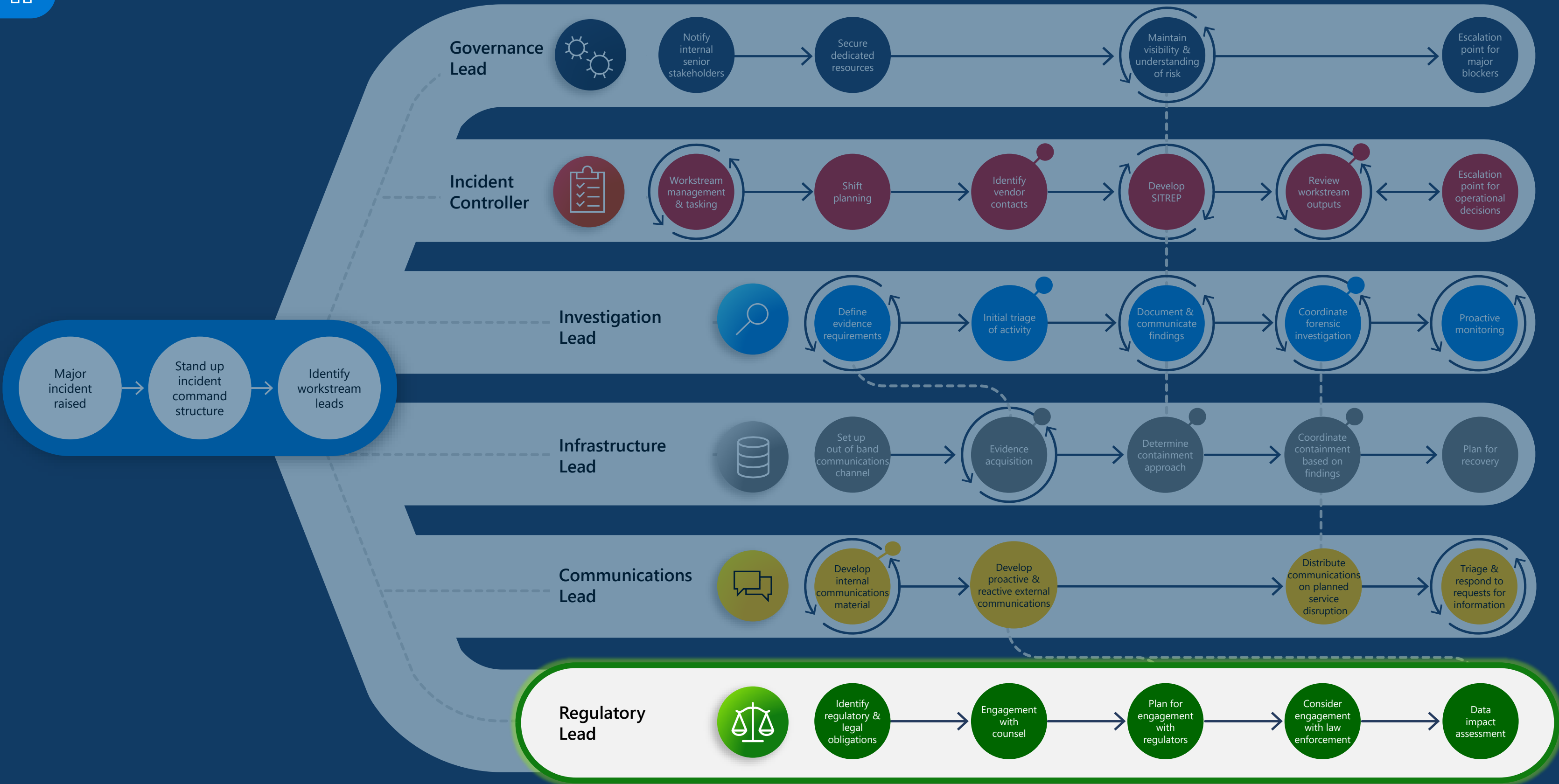
As a general rule, all communications on the incident should be approved by the Communications Lead to maintain consistency of messaging and a single source of truth on what is communicated to internal and external stakeholders who are not directly involved with the response.

Collaborating role:
[Regulatory Lead →](#)



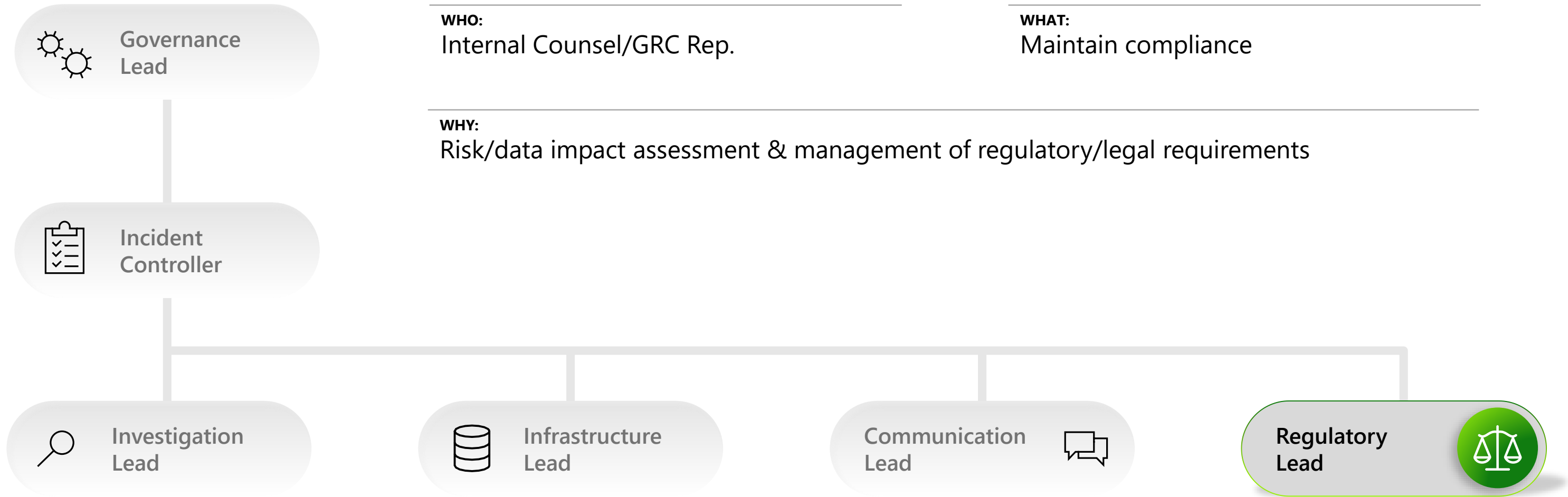
UP NEXT:

**Regulatory
Lead**





Regulatory Lead



Governance Lead



Incident Controller



Investigation Lead



Infrastructure Lead

Communication Lead



Regulatory Lead





Regulatory Lead



Identify regulatory and legal obligations

As incidents become more common, governments around the world are increasing regulatory oversight to keep pace. Understanding the specific regulatory and legal obligations which apply to your industry during an incident response is crucial.

Legal and regulatory obligations around cyber security incidents will differ between countries. It is best to consult legal counsel or GRC specialists.

Common pitfall

Organizations may delay engaging with government entities while trying to develop an understanding what happened. But keep in mind, there may be penalties for non-compliance with mandatory disclosure and privacy regulations. It is essential to know what you are expected to report, to whom, and by when.

This understanding can then be used to develop clear triggers for reporting—for example, if data exfiltration involving personally identifiable information is identified.

Common considerations include:



Mandatory reporting requirements to government cyber security authorities



Mandatory disclosure to a privacy commissioner or similar authority if personally identifiable information has been compromised



Regulatory reporting obligations if the incident causes impact to service delivery



Sector specific regulatory obligations, for financial institutions and operators of critical infrastructure



Regulatory Lead



Engagement with counsel

While engaging internal counsel, external counsel, or governance risk and compliance specialists at the outset of the response may not be front of mind, it is better to include these parties as early as possible to ensure they have the context required to provide support.

Counsel can provide valuable information on mandatory reporting and regulatory requirements and help you to navigate conversations with external parties. They may also be able to apply attorney client privilege to response artifacts.

In addition, counsel can assist in engagement with cyber insurers and law enforcement if required.

Common pitfall

Lack of early engagement with legal counsel can lead to unnecessary risk being introduced to the response. Without sound legal guidance, organizations may not meet their regulatory and compliance obligations, or perhaps overshare with external parties.



Collaborating role:
[Communication Lead](#) →



Regulatory Lead



Plan for engagement with regulators

Organizations must be aware of their regulatory obligations while managing an incident. Many countries now have mandatory reporting regulations for significant cyber incidents and require organizations to report on privacy breaches.

Organizations should understand the regulatory landscape and develop triggers for engagement with regulators to ensure compliance with the relevant laws and regulations.

Common pitfall

Often engagement with regulators is an afterthought during a major response. But many countries now have reporting time frames in place. Government entities may stipulate that notification of an incident must be provided a pre-defined number of hours after detection. Failure to meet these obligations may result in penalties or fines.





Regulatory Lead



Consider engagement with law enforcement

Law enforcement may be able to provide unique support through specific legal powers and authorities. Law enforcement may help with digital forensics, threat intelligence, and attribution.

In the event an organization has been extorted, law enforcement may also be able to assist with asset recovery.

Common pitfall

Organizations often miss opportunities by not engaging with law enforcement that can provide valuable support and insights, often beyond the capabilities of inhouse cyber security teams and vendors.





Regulatory Lead



Data impact assessment

During a cyber security incident, Threat Actors often seek to exfiltrate or even manipulate an organization’s data assets. If the investigation workstream has uncovered evidence of access to systems housing sensitive data, data staging or data exfiltration, organizations should work to understand the risk associated with this activity.

It is crucial to understand what data may have been exposed to the Threat Actor and the makeup of that data. This understanding may inform engagement with regulatory bodies, customers and other third parties, as well as recovery actions that may need to be taken.

Common pitfall

If a data impact assessment is not performed, organizations will not have a true understanding of the risk associated with the incident. For example, if the threat actor has accessed or exfiltrated technical documentation about IT systems, they may be able to access these systems in the future.

Similarly, a data impact assessment will help to uncover impact to personally identifiable information. This information can be used for second order targeting or extortion attempts against individuals.



Collaborating role:
[Communication Lead →](#)

Conclusion

By focusing first and foremost on the people and processes involved in incident response, organizations can avoid common pitfalls, clarify and plan for required roles, and manage responses efficiently, and people-centrally. This leads to more effective overall incident response.

Every incident is unique, but this information provides a scalable and adjustable plan to help organizations mitigate and minimize the impact of cybersecurity incidents.

