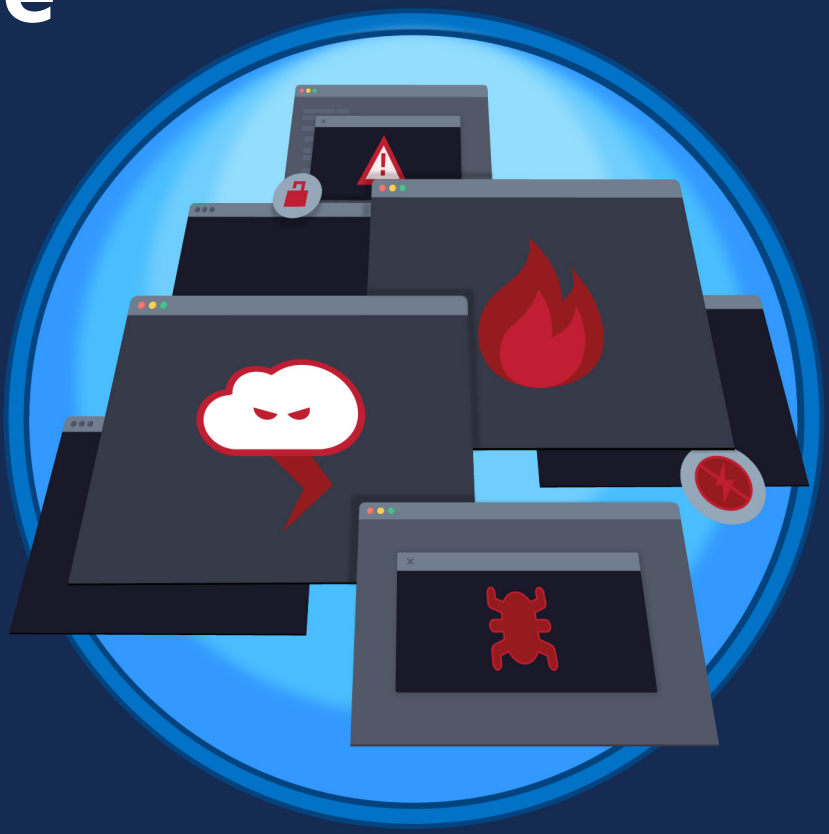
Cloud Incident Response Framework – A Quick Guide



cloud security alliance®

Acknowledgments

Initiative Lead:

Soon Tein Lim
Alex Siow

Key Contributors:

Christopher Hughes
Ashish Kurmi
Larry Marks
Michael Roza
Saan Vandendriessche

CSA Global Staff:

Jane Chow
Hing-Yan Lee
Haojie Zhuang

REVISION HISTORY		
Date	**Approval**	**Comments**
April 2020	John Yeoh	Original Publication
May 6th, 2020	Frank Guanco	Acknowledgments page updated

Table of Contents

1. Executive Summary

Cyber risk exposure for an organization is a daily concern. Organizations regularly worry about cyber risk exposure to their IT infrastructure or data breaches, which as a result, could end in large penalties or outages. These cyber-threats are commonly caused by malicious attacks, misconfigurations, or even disgruntled employees. Any of which could easily cripple entire businesses, resulting in extensive reputational and financial repercussions. Major incidents serve as painful reminders of the fallout such occurrences can cause.

In today's connected era, a comprehensive incident response strategy is an integral aspect of any organization aiming to manage and lower their risk profile. A good incident response strategy needs to be useful not only when dealing with incidents caused by malicious threat actors, but should also be applicable in a variety of other situations such as downtime caused by an unexpected power outage or cut internet fiber due to roadworks. There are, however, different considerations when it comes to incident response strategies for cloud-based infrastructure and systems, due in part to the nature of its shared responsibility.

Standards bodies, government agencies, cloud service providers (CSPs), research institutes and security experts have developed various incident response frameworks and best practices to help organizations be better prepared when dealing with cloud incidents. These frameworks and best practices provide methodical, step-by-step response plans to various types of cloud incidents, which in turn, help manage and minimize damage to businesses.

With the abundance of Cloud Incident Response (CIR) standards, frameworks and guidelines available in the industry, CSA's CIR Working Group (WG) aims to provide a holistic and consistent view across widely used frameworks for the user, be it CSPs or cloud customers. Ultimately, the WG hopes to develop a holistic Cloud Incident Response (CIR) framework that covers the major causes of cloud incidents (both security and non-security related), and their handling and mitigation strategies. The aim is to serve as a go-to guide for cloud users to effectively prepare for and manage the aftermath of cloud incidents, along with serving as a transparent and common framework for CSPs to share cloud incident response practices with their customers.

This Quick Guide distills the main objectives and gives readers an overview of the key contributions and efforts currently underway inside the CIR WG. As we move towards a comprehensive CIR framework, the CIR WG hopes to take this opportunity to encourage volunteers to participate in the WG's efforts and provide valuable feedback to the ongoing work.

2. Introduction

2.1 Incident Response vs Cloud Incident Response

> NIST's Definition of Incident[1]
>
> An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Migrating systems to the cloud is not a lift-and-shift process – which also applies to the Incident Response (IR) process. Cloud is a different realm altogether, and expectedly, CIR is too. The three key aspects that set CIR apart from traditional IR processes are governance, visibility, and the shared responsibility of the cloud.

Governance

Data in the cloud resides in multiple locations, sometimes with different CSPs. Getting the various organizations together to investigate an incident is a major challenge and can be resource draining on large CSPs that have a colossal client pool.

Shared responsibility

Cloud customers, CSPs and/or third-party providers all have different roles to play when ensuring security in the cloud. Generally, customers are responsible for their own data, while CSPs are responsible for the cloud infrastructure and services that they provide. CIR should always be coordinated across all parties.

It is important to discuss in granular detail with your CSP to ensure that the roles and governance are clear. Be sure not to create or settle for any policy that you are unable to enforce. Organizations should understand that they can never outsource governance or shared responsibilities.

Visibility

Lack of visibility in the cloud indicates that incidents that could have been resolved quickly are now at risk of escalating. The cloud has the benefit of ensuring an easier, faster, cheaper and more effective IR when leveraged properly. It is important to take great care when developing IR processes and documentation, taking full advantage of cloud architectures as opposed to traditional data center models. Many tools, services, and capabilities provided by CSPs greatly enhance detection, reaction, recovery and forensic abilities that are curated for, and only possible in the cloud. CIR has to be proactive and architected for failure throughout the process.

[1] NIST Computer Security Resource Center, Glossary - Incident, https://csrc.nist.gov/glossary/term/incident

2.2 What This Quick Guide Does

The CIR Framework provides a more detailed look into each of the subsequent chapters covered in this Quick Guide. The CIR Framework focuses on and should be applicable to all cloud incidents. These incidents can be a result of both security and non-security related events, including but not limited to operational mistakes, infrastructure or system failure, natural disasters, distributed denial of service (DDoS) and phishing attacks. The CIR Framework not only provides guidelines on developing an effective incident response procedure, but has a more underlying purpose of addressing the detection, analysis, and handling of incidents. The framework is intended to help cloud users choose the appropriate level of incident protection to complement their Business Continuity/Disaster Recovery capabilities. It's goal is to enable CSPs to align to market demands around service expectations, and to allow regulators to standardise Business Continuity Management (BCM) requirements for CSPs.

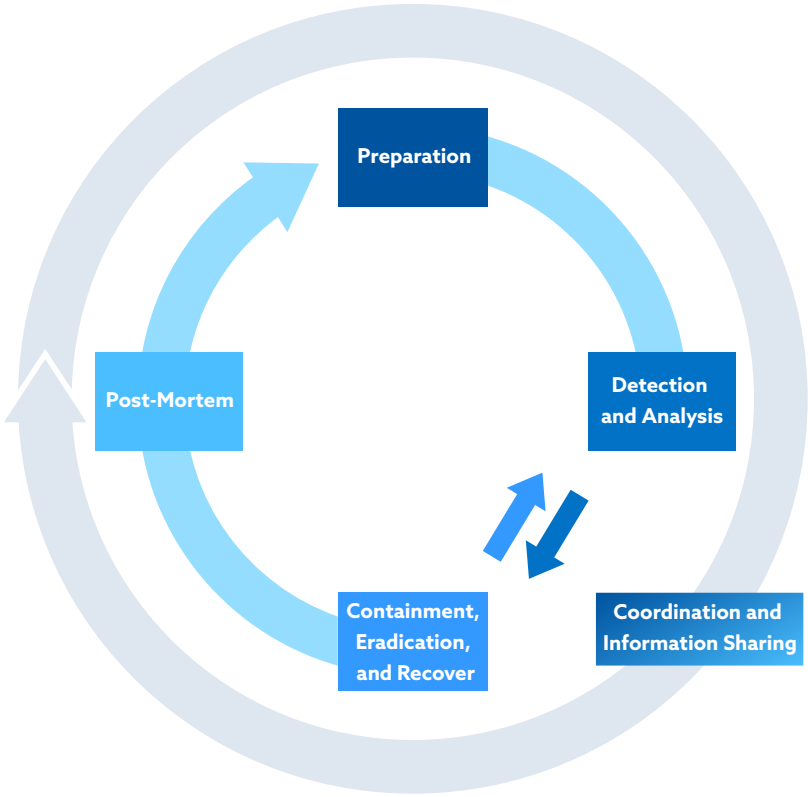
Through this quick guide, we hope to highlight the essence of the CIR so readers can expect more comprehensive coverage in the upcoming CIR Framework. The CIR WG also hopes to take this opportunity to call for any contributors interested in developing the framework with the community.

2.3 How Everything Kind of Fits Together

The CIR Framework refers to several industry-accepted standards and frameworks to plan and prepare for cloud incident, mitigation strategies and post-mortem processes. The current list is not exhaustive, and the CIR WG welcomes contributions from the public.

1. Technical Reference (TR) 62 – Cloud Outage Incident Response (COIR)
2. CSA Security Guidance For Critical areas of Focus In Cloud Computing v4.0
3. NIST 800-61 Computer Security Incident Handling Guide
4. ISO/IEC 27035-1:2016
5. ENISA Cloud Computing Risk Assessment
6. Other relevant documents:
    - ISO 22320:2011 Societal Security - Emergency Management - Requirements for Incident Response
    - FedRAMP Incident Communications Procedure
    - NIST 800-150 Guide to Cyber Threat Information Sharing
    - NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
    - SANS Institute Information Security Reading Room Incident Handler's Handbook

There is an abundance of Incident Response (IR) standards, frameworks and guidelines available in the industry today, which can be overwhelming for organizations to comprehend. The following IR lifecycle diagram provides a clear understanding of how various chapters and sections across different frameworks fit into an IR lifecycle. This is especially helpful when the user needs to zoom in and plan for specific phases in the response process.



Preparation	Detection and Analysis	Containment, Eradication and Recovery	Post-Mortem	Coordination and Information Sharing
NIST 800-61r2 3.1 Preparation	**NIST 800-61r2** 3.2 Detection and Analysis	**NIST 800-61r2** 3.3 Containment, Eradication and Recovery	**NIST 800-61r2** 3.4 Post-Incident Activity	**NIST 800-61r2** 4 Coordination and Information Sharing
TR 62 0.1 Cloud Outage Risks	**TR 62** 4.2 COIR Categories 5.1 Before Cloud Outage (CSCs) 6.1 Before Cloud Outage (CSPs)	**TR 62** 5.2 During Cloud Outage (CSCs) 6.2 During Cloud Outage (CSPs)	**TR 62** 5.3 After Cloud Outage (CSCs) 6.3 After Cloud Outage (CSPs)	**FedRAMP Incident Communication Procedure** 2 Stakeholder Communications
FedRAMP Incident Communication Procedure 5.1 Preparation	**FedRAMP Incident Communication Procedure** 5.2 Detection and Analysis	**FedRAMP Incident Communication Procedure** 5.3 Containment, Eradication and Recovery	**FedRAMP Incident Communication Procedure** Post-Incident Activity	**NIST (SP) 800-53 r4** Appendix F-IR IR-4, 1R-7, IR-9
NIST (SP) 800-53 r4 3.1 Selecting Security Control Baselines Appendix F-IR IR-1, 1R-2, 1R-3, IR-8	**NIST (SP) 800-53 r4** Appendix F-IR AT-2, 1R-4, IR-6, 1R-7, IR-9, SC-5, SI-4	**NIST (SP) 800-53 r4** Appendix F-IR 1R-4, IR-6, IR-7, IR-9	**CSA Security Guidance v4.0** 9.1.2.4 Post-mortem	**NIST (SP) 800-150** 4 Participating in Sharing Relationships
CSA Security Guidance v4.0 9.1.2.1 Preparation	**CSA Security Guidance v4.0** 9.1.2.2 Detection and Analysis	**CSA Security Guidance v4.0** 9.1.2.3 Containment, Eradication and Recovery	**The Incident Handlers Handbook** 7 Lessions Learned 8 Incident Handlers Checklist	
ENISA Cloud Computing Security Risk Assessment Business Continuity Management, page 79	**The Incident Handlers Handbook** 3 Identification 8 Incident Handlers Checklist	**The Incident Handlers Handbook** 4 Containment 5 Eradication 6 Recovery 8 Incident Handlers Checklist		
The Incident Handlers Handbook 2 Preparation 8 Incident Handlers Checklist				

3. CIR Framework

The ninth domain of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0[2] is CIR. CIR is a key pillar to robust and reliable information security. An effective CIR framework – one that is tailored for cloud – can help prepare your organization to mitigate such risks when disaster strikes.

The Incident Response Lifecycle defined in the NIST 800-61rev2 document includes the phases *Preparation*, *Detection and Analysis*, *Containment*, *Eradication*, and *Recovery*, and lastly, *Post Mortem*. *Coordination and Information Sharing* is continuous and should occur across all phases of the lifecycle.

3.1 Phase 1: Preparation

> Preparation: "Establishing an incident response capability so that the organization is ready to respond to incidents."[3]

Solid preparation can improve an incident response team's readiness and efficiency, ensuring they are sufficiently prepared in the face of threats. Organizations should work towards having more than one mechanism in place to avoid single points of failure.

A good CIR plan should clearly establish everyone's roles and responsibilities. A list of emergency contacts and the various methods of communications should also be ready for reaching out to key parties within or beyond the organization for assistance. If third-party IR providers are engaged, the CIR plan should be around your third-party vendors. During the preparation phase, organisations should consider vetting any third-party IR providers to have quick access to resources, should they be needed in an emergency response situation.

Because every cloud platform is slightly different, there is no one-size-fits-all CIR plan. One concept to consider is Chaos Engineering[4], the goal of which is to build more resilient systems by *experimenting on a system in order to build confidence in the system's capability to withstand turbulent conditions in production*.

In addition to offline backups, organizations should make full use of their CSPs' business continuity and disaster recovery capabilities, and be familiar with them so they can invoke them in the event of incidents.

---

[2] Cloud Security Alliance 2017, Security Guidance for Critical Areas of Focus in Cloud Computing v4, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[3] Cloud Security Alliance 2017, Security Guidance for Critical Areas of Focus in Cloud Computing v4, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[4] Chaos Community Google Group 2018, Principles of Chaos Engineering, https://principlesofchaos.org/?lang=ENcontent

CIR plans should be tested through mock incident scenarios and exercises as part of staff training and ideally be reviewed and updated with every use as part of Post-Mortem efforts, or at least annually. CIR can be stressful when assets are at stake, thus having a solid CIR plan already in place can help to reduce critical mistakes, improved preparedness, efficiency, and responsiveness.

3.2 Phase 2: Detection and Analysis

> Detection and Analysis: Detection, confirmation, and analysis of suspected incidents;[5]

Although detection and analysis may differ from one cloud environment to the other, the monitoring scope must cover the cloud management plane in addition to deployed assets. In-cloud monitoring and alerts can be leveraged to help kick off an automated response workflow. Cloud logs (which might not be available for all CSPs, or across all service models of SaaS, PaaS and IaaS), preferably complete logging of all management activities and API calls, can help to address questions such as:

- When did it happen? Who discovered it and how was it discovered?
- Have any other areas been impacted, and what is the confidence level for the non-impacted zones?
- Has the source or patient zero been discovered?

Incident Classification Scale

Incident classification scales are used in several industry best practices and guidelines to help users gauge the severity of impact and/or the relative importance of cloud services availability to business operations. The WG is developing an Incident Classification Scale of 5 categories, from Level 1 to Level 5, with impact-increments at each level. Listed below are some mappings which are to be expected in the subsequent deliverable, CIR Framework:

- ENISA Cloud Security Incident Reporting
- NIST Computer Security Incident Handling Guide
- TR 62 Guidelines for Cloud Outage Incident Response

[5] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

	Level 1		Level 2	Level 3	Level 4	Level 5
ENISA	**Impact 0** Something went wrong an excercise or a test. No impact on users.	**Impact 1** Incident had impact on assets, but no direct impact on customers.	**Impact 2** Incident had impact on assets, but only minor impact on customers.	**Impact 3** Incident had impact on customers.	**Impact 4** Incident had major impact on customers.	
NIST (Functional Impact)	**None** No effect to the organizations's ability to provide all services to all users	**Low** Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	**Medium** Organization has lost the ability to provide a critical service to a subset of system users		**High** Organization is no longer able to provide some critical services to any users	
NIST (Information Impact)	**None** No effect to the organizations's ability to provide all services to all users		**Privacy Breach** Surisitive porsunally identifiable information (PII) of taxpayers. employees, beneficiaries, etc. was accessed or exfiltrated **Proprietary Breach** Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated **Integrity Loss** Sensitive or proprietary information was changed or deleted			
TR 62	**Category D - Minimal impact** A category of cloud services that is least important to the operations of an organisation Alternative means or fall-back mechanisms are readily available or long duration of outage in days is tolerable and access to data is not urgent during this period.		**Category C - Operational impact** A category of cloud services that is essential to the operations of an organisation. The organisation's operations are usually restored within 24 h and have a medium urgency to access data during this period or else outage would significantly impact the organisation's operational efficiency and effectiveness.		**Category 8- Business critical impact** Impact business severely. The organisation's operations are restored within hours, during which data access is urgent and survival is at stake if the outage is prolonged.	**Category A - Systemic/ mission critical impact** The impact is beyond an organisation's operations and any outage will put human safety or the stability of market economy or industry at stake.

Table 1. Example of Table with Mapping of Incident Severity Level to Relevant Frameworks

3.3 Phase 3: Containment, Eradication, and Recovery

> Containment & Eradication: Minimizing loss, theft of information, or disruption of service, and elimination of the threat;
> Recovery: Restoring the computing services securely and in a timely manner;[6]

When an incident is discovered, predefined CIR plans as stipulated in Phase 1, Preparation, should be executed (eg. taking systems offline, quarantining systems, restricting connectivity). It is of the utmost importance not to remove the threat by blind deletion as this is equivalent to destroying evidence which is required for forensics and revising the CIR plan. The key is to be meticulous in removing any tiny trace of malware, threats or issues. It is also important to evaluate the compromise of data loss versus service availability. To prevent incidents from reoccuring, systems should be hardened and patched following an immutable infrastructure paradigm. This means servers are never modified after deployment and any changes or fixes are built into a new image that replaces the old one.

Whenever possible, make full use of cloud backups, mirroring or restoration services provided by your CSPs for a quick and seamless recovery. These CSP and cloud-centric services can often ensure a more robust recovery (tailored for cloud) compared to traditional on-prem or third-party solutions.

The working group aims to develop containment, eradication, and recovery guidelines that are specific to each level in the Incident Classification Scale. This will be published in the subsequent deliverable by the CIR WG. Individuals who are interested in participating in this work may join the WG here.

3.4 Phase 4: Post-Mortem

> Post-Incident Activity: Assessment of the incident response to better handle future incidents through the utilization of logs review, "Lessons Learned" and after-action reports, or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.[7]

Once the storm is over, the IR team should gather to analyse and document the incident and determine what went well and what could be improved. The lessons learned will help in revising and solidifying the CIR plan. The post-mortem phase is essential, and should be performed as soon as possible, while the lessons are still fresh in everyone's mind. Important details may be lost or forgotten which could make a valuable difference in preventing a future incident.

3.5 Continuous Phase: Coordination and Information Sharing

Communication between the provider and the users needs to be properly established. Regular updates should be available for affected users to mitigate losses and strategize business recovery methods.

[6] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf
[7] FedRAMP PMO 2017, FedRAMP Incident Communication Procedure, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

Effective coordination goes beyond just reporting to the customers. An attack typically affects more than one organization simultaneously. Thus incident information sharing is mutually beneficial in helping other organizations guard against the same threats. The CSA runs the Cloud Cyber Incident Sharing Center (CloudCISC)[8] that facilitates the sharing of incident data between participating CSPs.

Coordinating with key partners, IR teams in other departments, law enforcement agencies on their specific roles and responsibilities greatly reinforce CIR capabilities. This communication should be set up from the start – at the planning phase – and maintained throughout the entire CIR process when necessary.

4. Incident Response Controls

As with all frameworks (including the CIR Framework), security controls are best implemented during creation and not as an afterthought, as something extra to be tacked on only because it is required. The CIR Framework, implemented correctly, will reduce the risk and uncertainty of incidents by ensuring the organization is prepared to deal with the consequences of an attempted (or successful) breach of security.

The IR Phases discussed above are mapped at a high level in Chapter 7 in the upcoming CIR Framework document to the incident response sections for five of the most well-known cloud security standards (CSA CCM, FedRAMP, NIST, ISO, and CIS). This suggests that if the CSA CIR Framework is used as a basis for creating an IR System, that system should comply at least partially with these well-known standards. Detailed mappings (with the exception of CIS) can be found in the CSA CCM Cloud Matrix 3.01 Full Version[9]. The CCM and these mappings are important for complying with the CSA Security Trust Assurance and Risk (STAR) Certification[10].

5. Conclusion

In the event of a critical incident, there is no time to waste figuring out a game plan - every second that goes by puts data at risk of being potentially compromised. The CSA CIR WG is developing a sequel to this document, the Cloud Incident Response Framework, which delves into each chapter in greater depth. Readers can expect a step-by-step guide, from preparation to post-mortem, with CIR guidelines curated for different levels of incident severity. Key ideas and concepts are covered in each phase and should apply to all cloud incidents.

As a work in progress, the CIR WG welcomes individuals who are interested in contributing to this work to join the WG by registering here.

[8] More information on CloudCISC: https://cloudsecurityalliance.org/research/working-groups/cloud-cisc/

[9] More information on CSA CCM: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

10 More information on CSA STAR: https://cloudsecurityalliance.org/star/