

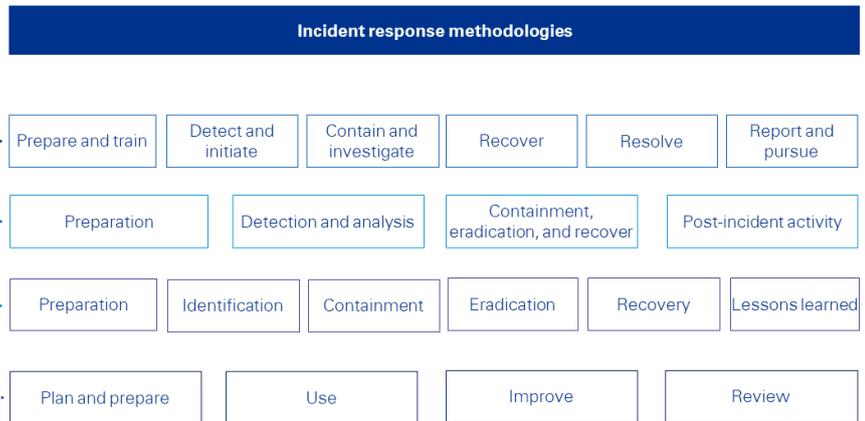
# On-demand Cyber Response Services

## Cyber | Cyber Response Services

KPMG Forensic / Tech Assurance

In the unpredictable and fast-paced battle against cyber attackers, well-prepared incident response teams are a powerful weapon in an agency's arsenal. Responsible for assessing security systems and responding to security threats, incident response teams play a vital role in resolving issues and controlling the damage of system breaches, malware exposure, and other security events.

KPMG's approach to Cyber Response is created in accordance with several internationally acceptable frameworks including NIST, ISO, and SANS. Our approach is refined through real-world experiences with a focus on actionable results, rules of evidence, and technical security experience.



### Prepare and Train

One of the most common causes of a failed response is a lack of adequate preparation. KPMG can assist your organisation in establishing clear lines of communication, policies, procedures, and rules of engagement, in order to set the groundwork for a successful response if and when an incident occurs. In a parallel track, our teams work continuously to keep current on the latest technical methods, tools, and certifications for incident response.



### Detect and Initiate

The trigger for this phase is a technical alert, an indication of fraud, or other communications from an outside entity such as law enforcement or an Internet service provider to your organisation. Our incident response professionals help execute plans created during the preparation phase and provide answers to pressing questions, such as: Have we been breached? Is the activity continuing? What are the potential damages? Do we need to begin notification and self-reporting?



### Contain and Investigate

During this phase, we help determine the source, method, and impact of the breach event, while attempting to assist you in limiting ongoing damage. These efforts are typically a balancing act between investigating and eradicating the threat. Responses can range from allowing the malicious actions to continue in order to facilitate evidence-gathering to an immediate suppression of malicious actions in order to limit the damage.



### Recover

This phase consists of removal efforts that could not occur during the previous phases because of the potential impact on investigative efforts or prioritisation of other activities. The focus of this stage is to return the environment to normal operations.



### Resolve

A significant work stream during this phase is vulnerability assessment and penetration testing. This work may occur throughout the incident response process to support tactical efforts and is followed by a more comprehensive process during this phase in order to determine the root causes of the malicious activity. This enables us to produce prioritised recommendations for improving the technical and governance environments, which can help prevent similar events from occurring in the future.

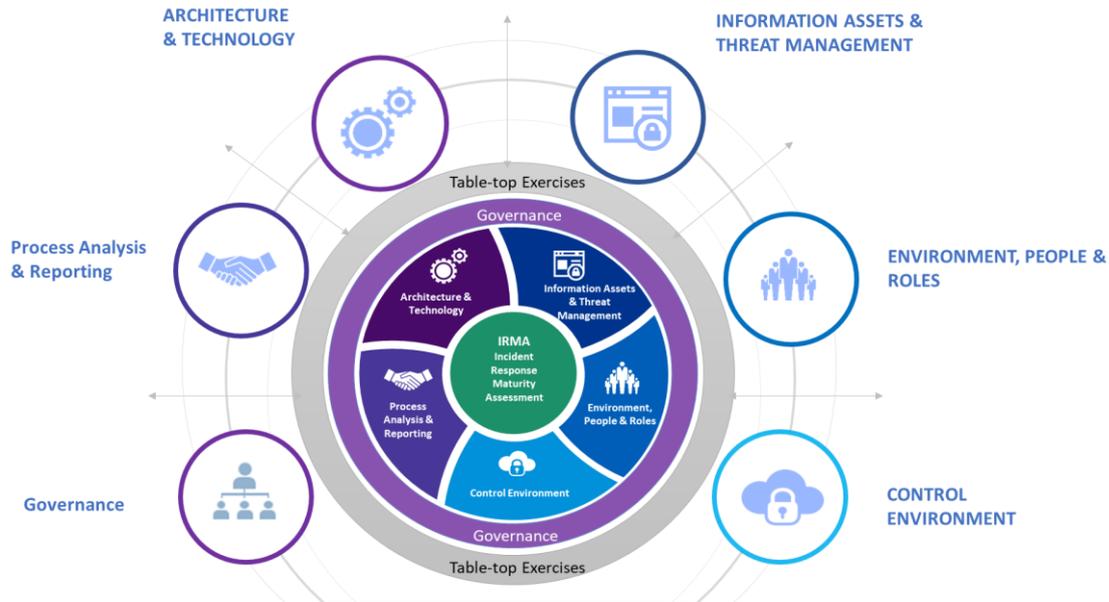


### Report and Pursue

The final phase consists of engagement reporting and may include ongoing support activities related to the legal or civil pursuits of individuals or groups.

# Cyber Incident Response Maturity Assessment (IRMA)

In line with our proactive approach to cyber incident response, consideration should also be given to the Incident Response Maturity Assessment (IRMA). KPMG's IRMA provides an in-depth review of an organisation's ability to respond to Cyber security incidents its information assets and its readiness against cyber-attack and consequences. It is exceptional in the market in that it looks beyond pure technical preparedness against cyber security incidents. It takes a rounded view of people, processes, and technology to enable clients to understand areas of vulnerability, identify and prioritize areas for remediation, and demonstrate both corporate and operational compliance, turning an incident response into a business advantage. We are able to measure client incident response maturity according to the types of data assets, the industry approach, a variety of geographies, and the regulatory and legislative requirements of each location.



## How can we engage?

KPMG, with its experience of working with several clients and being rated as a leader in cyber security, is well positioned to meet client objectives and create a resilient first responder mechanism. The following is our custom-built cyber response service model:



### Key differentiators of KPMG Cyber Response capabilities:

- 24 X 7 monitored Cyber Hotline
- Qualified and experienced team of field responders
- Coverage across multiple regions in Africa
- Access to KPMG global learning base
- Availability of SMEs for professional advice on specific forensic matters
- Custom delivery models to optimize expenses
- Stand-by team of forensic experts for detailed investigation and litigation support
- Agile yet effective onboarding, if required
- Hub and be-spoke model with a central PMO for simple effective execution and seamless communication

## Contact us



**Rupesh Vashist**  
**Director, Tech Assurance**  
**T: +27 (66) 101 6590**  
**E: rupesh.vashist@kpmg.co.za**



**Sameer Vyadally**  
**Role**  
**T: +27 (66) 010 7878**  
**E: sam.vyadally@kpmg.co.za**

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



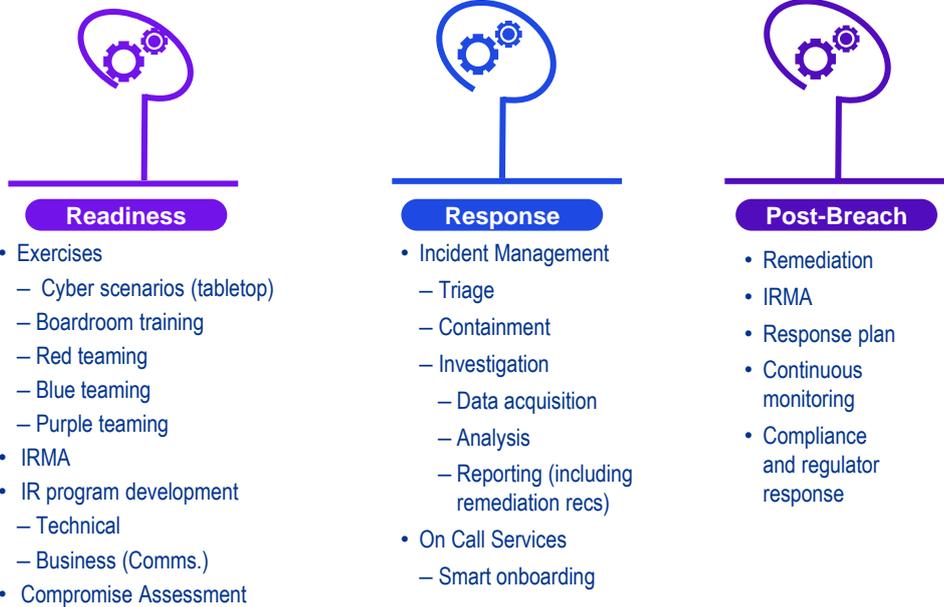
© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

© 2022 KPMG Services (Pty) Limited, a South African company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

For more detail about our structure, please visit [home.kpmg/governance](https://home.kpmg/governance).

## Summarising Our Incident Response Services



## Summarising Our Cyber Security Services

The table below summarises our Cyber Security offerings.

Strategy and governance	Transformation	Cyber defense	Cyber response
Helping clients understand how best to align their cyber agenda with their dynamic business and compliance priorities	Helping clients build and improve their programs and processes, supported by the right organization and technology, to improve their cyber agenda	Helping clients maintain their cyber agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks	Helping clients effectively and efficiently respond to cyber incidents and conduct forensic analysis and detailed investigations



**Cyber Security Services** sees the world from the client's perspective, bringing a business context to cybersecurity for all levels of the organization, from the boardroom to the back office.

We help organizations in transforming their security function into business-enabling platforms so they can understand, prioritize, and manage their cybersecurity risks, take control of uncertainty, increase agility, and convert risk into an advantage.

### Contact us



**Déan Friedman**  
Director/Head of Forensic

T: +27 (82) 719 0336

E: dean.friedman@kpmg.co.za



**Rupesh Vashisht**  
Director, Tech Assurance

T: +27 (66) 101 6590

E: rupesh.vashist@kpmg.co.za



**Sameer Vyadally**  
Associate Director, Tech Assurance

T: +27 (66) 010 7878

E: sam.vyadally@kpmg.co.za

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

© 2022 KPMG Services (Pty) Limited, a South African company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

For more detail about our structure, please visit [home.kpmg/governance](https://home.kpmg/governance).