The Incident Response Plan That Saved Christmas

Petra Smith
Aura Information Security

Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

DATACOM

QUANTUM
SECURITY

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

myob

Pulse Security
www.pulsesecurity.co.nz

VOCUS

LATERAL
SECURITY

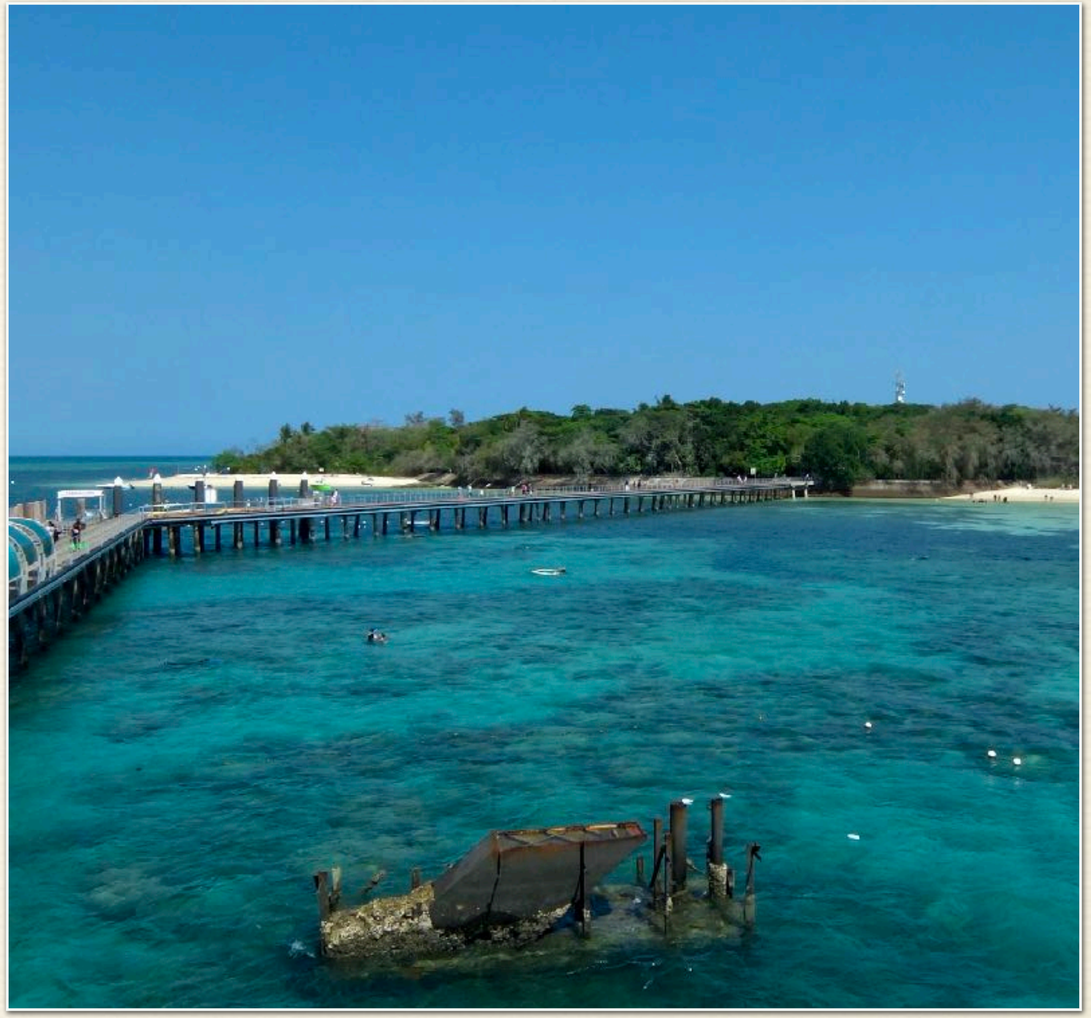
SEQA™
Information Security

Without them, this Conference couldn't happen

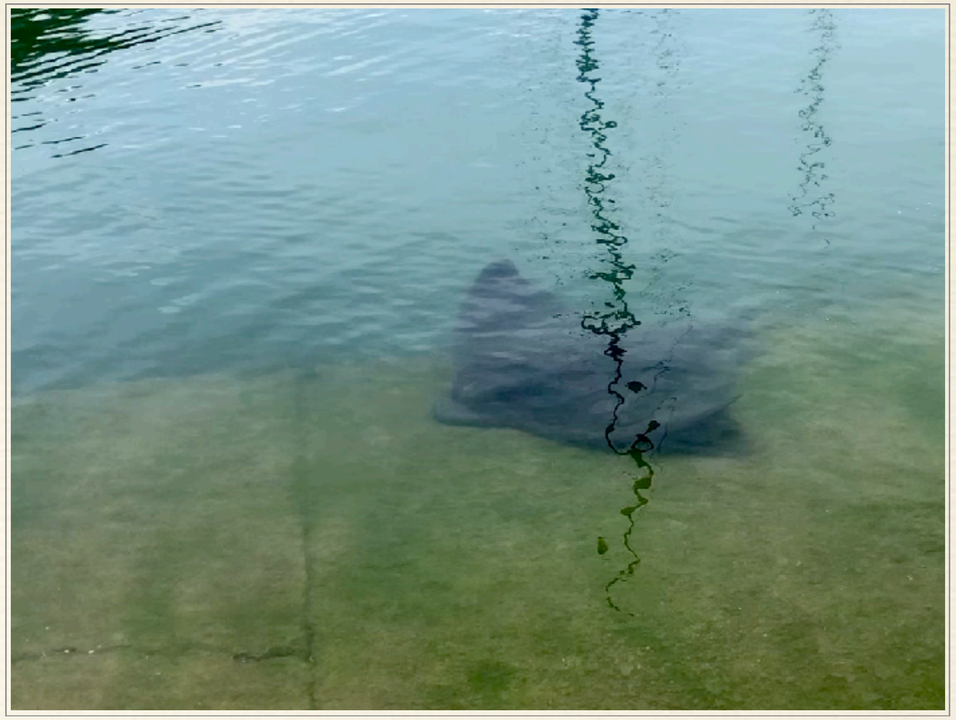
Yidindji Country

Far North Queensland

December 2019

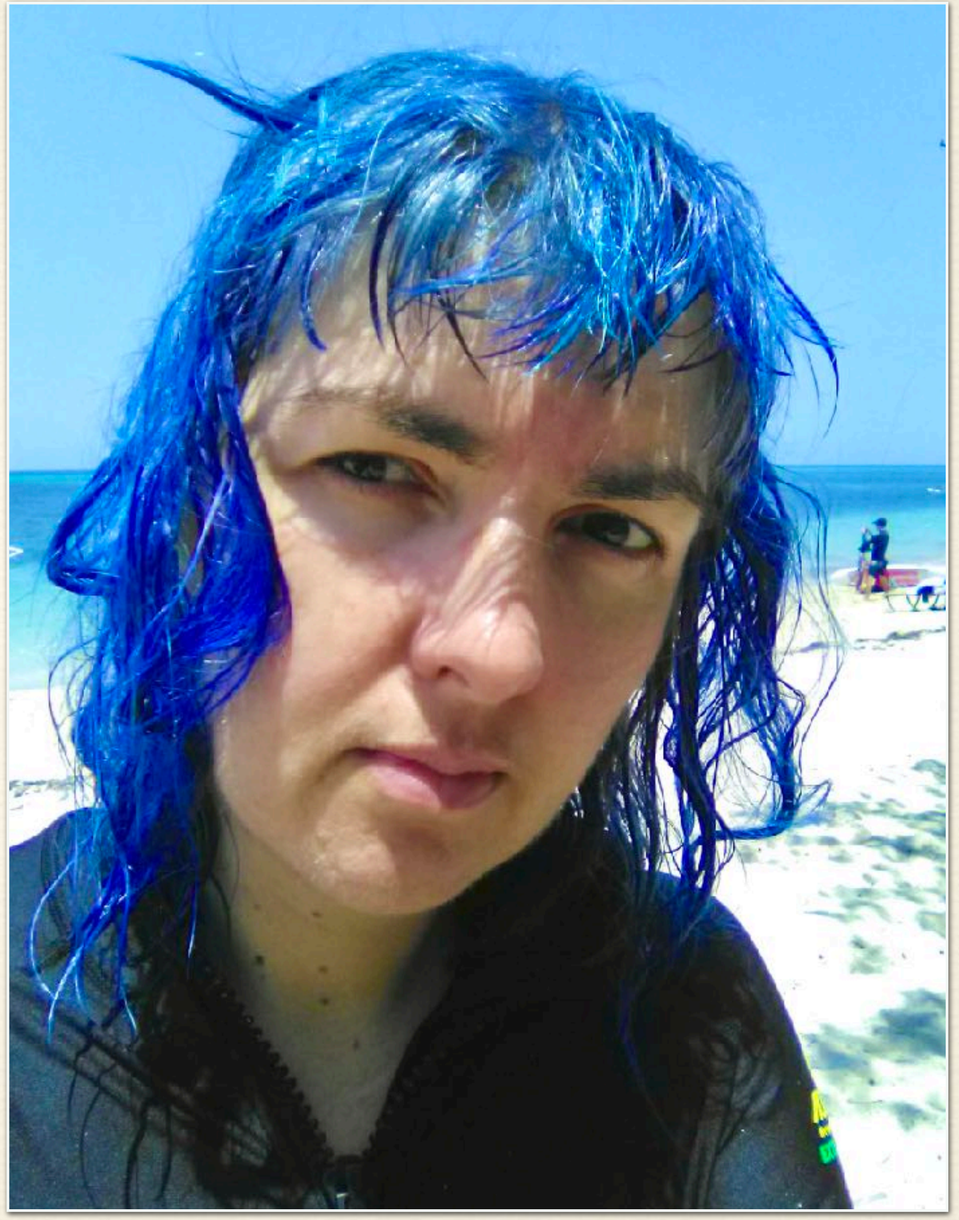


Fitzroy Island postcard (fish not to scale)




WARNING
ACHTUNG
警告
Crocodiles inhabit this area attacks may cause injury or death
Keep away from the water's edge and do not enter the water.
Take extreme care when launching and retrieving boats.
Do not clean fish or leave fish waste near the water's edge.
Camp well away from the water.


WARNING
STINGERS



Approaching Fitzroy Island

Indo-Pacific Seargent (*Abudefduf vaigiensis*)

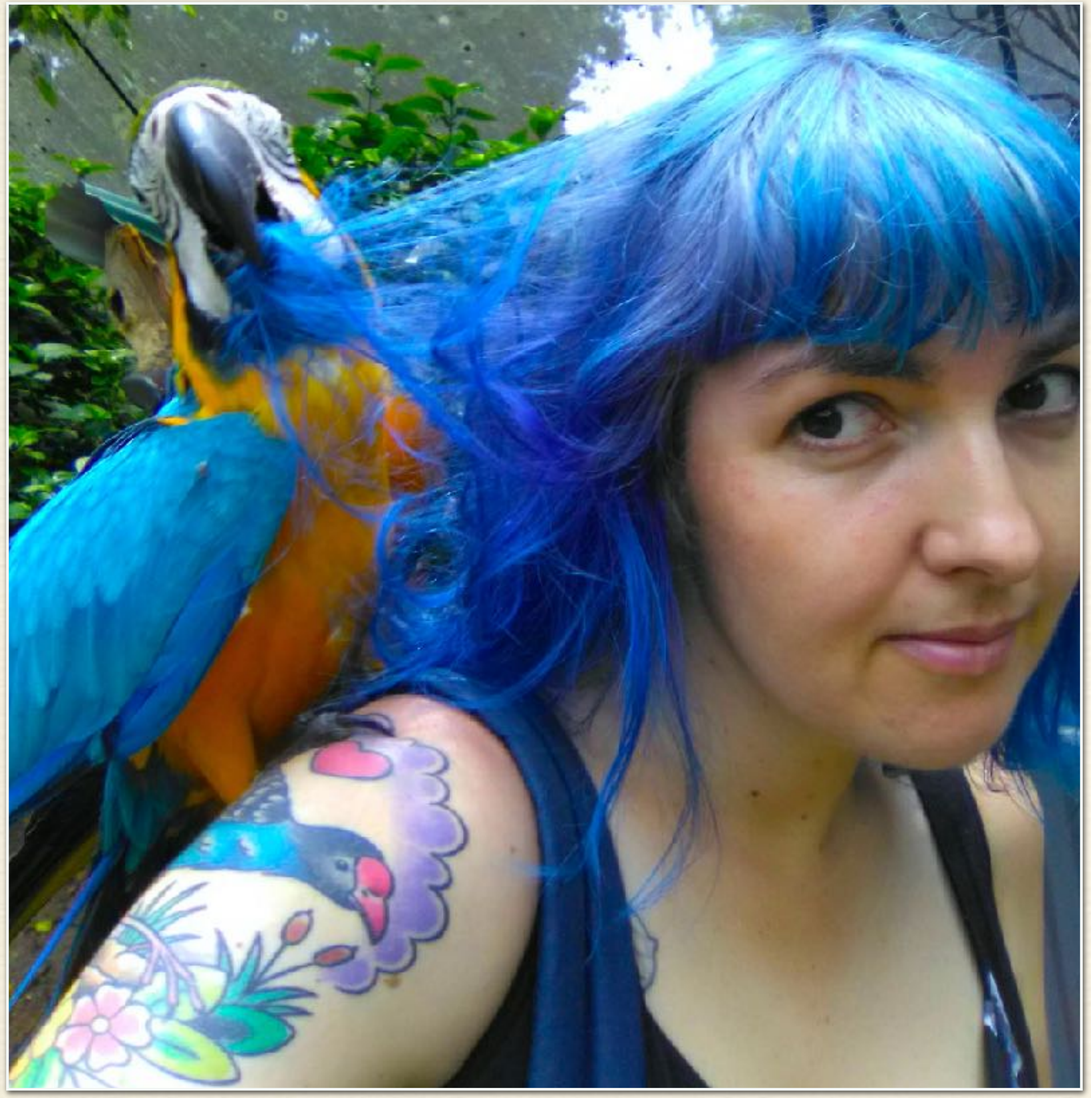
Various hard corals

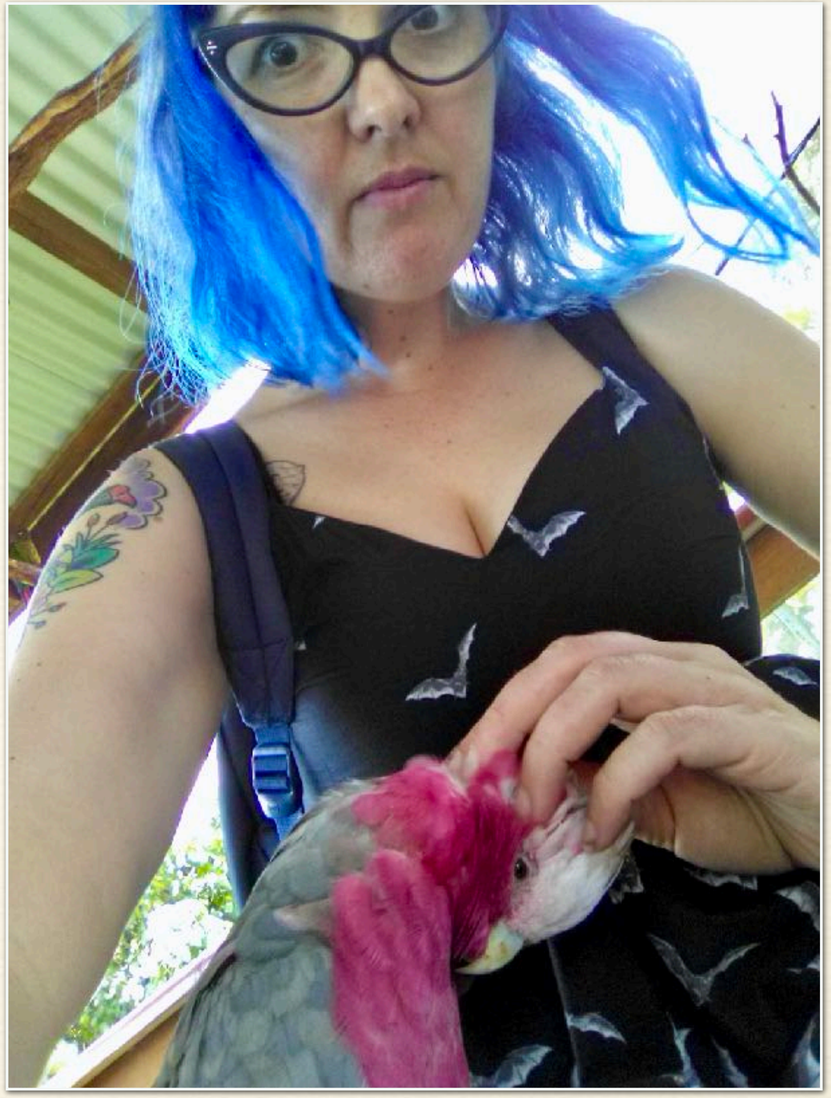
Soft coral colony

Giant clams (*Tridacna gigas*)

Box jellyfish by Alexandra Roberts
(flickr.com/photos/threemilesdwn/3609828652)

Green turtle (*Chelonia mydas*)





Making friends at the Kuranda free-flight aviary

Scissortail damselfish (*Abudefduf sexfasciatus*)

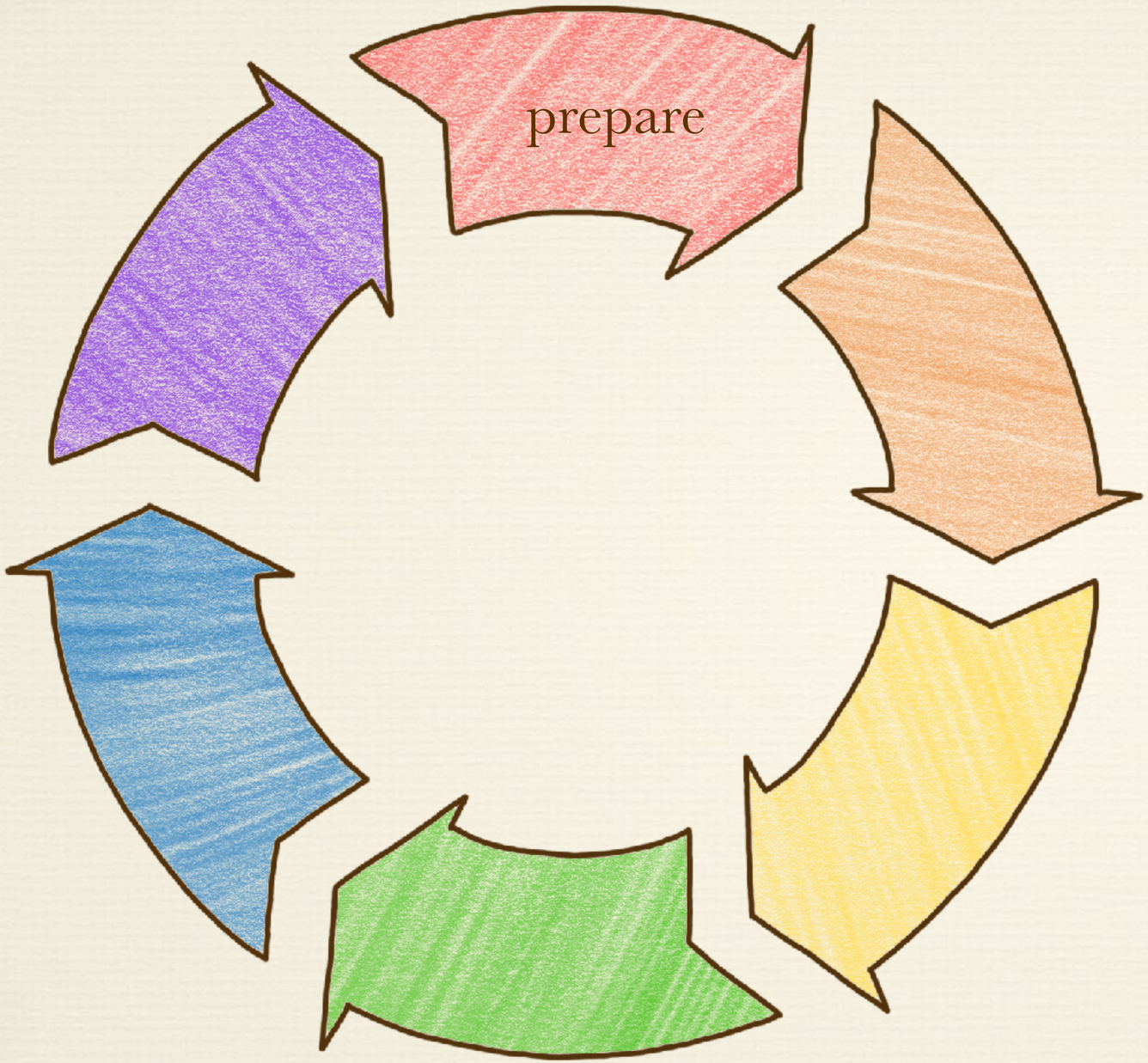
An Incident Response Plan is your guidebook to unknown territory.

“We don’t need a plan – if anything happens we’ll just put everyone in a room and figure out what to do.”

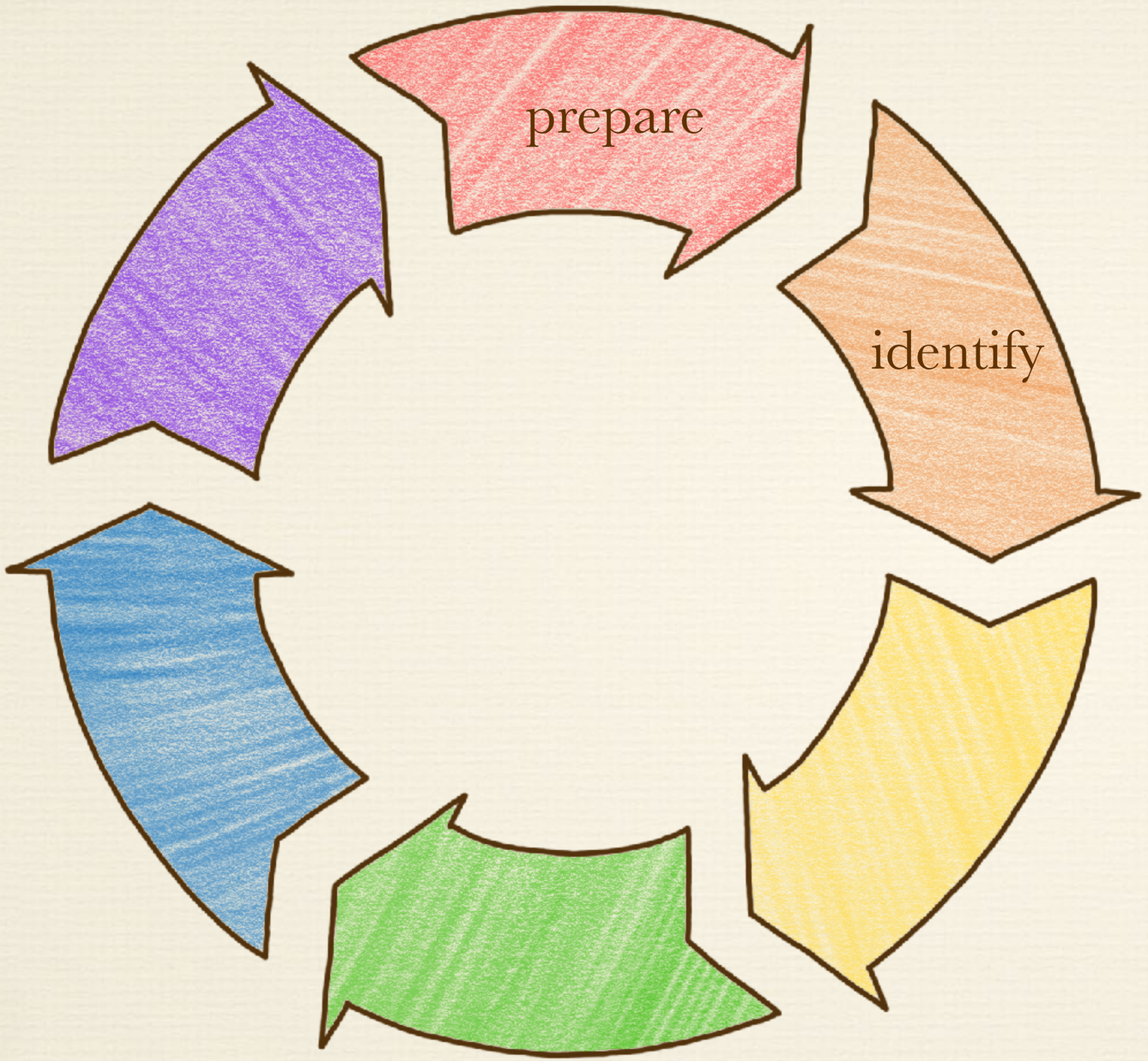
traditional dev team proverb

Do I *really* need an IR Plan?

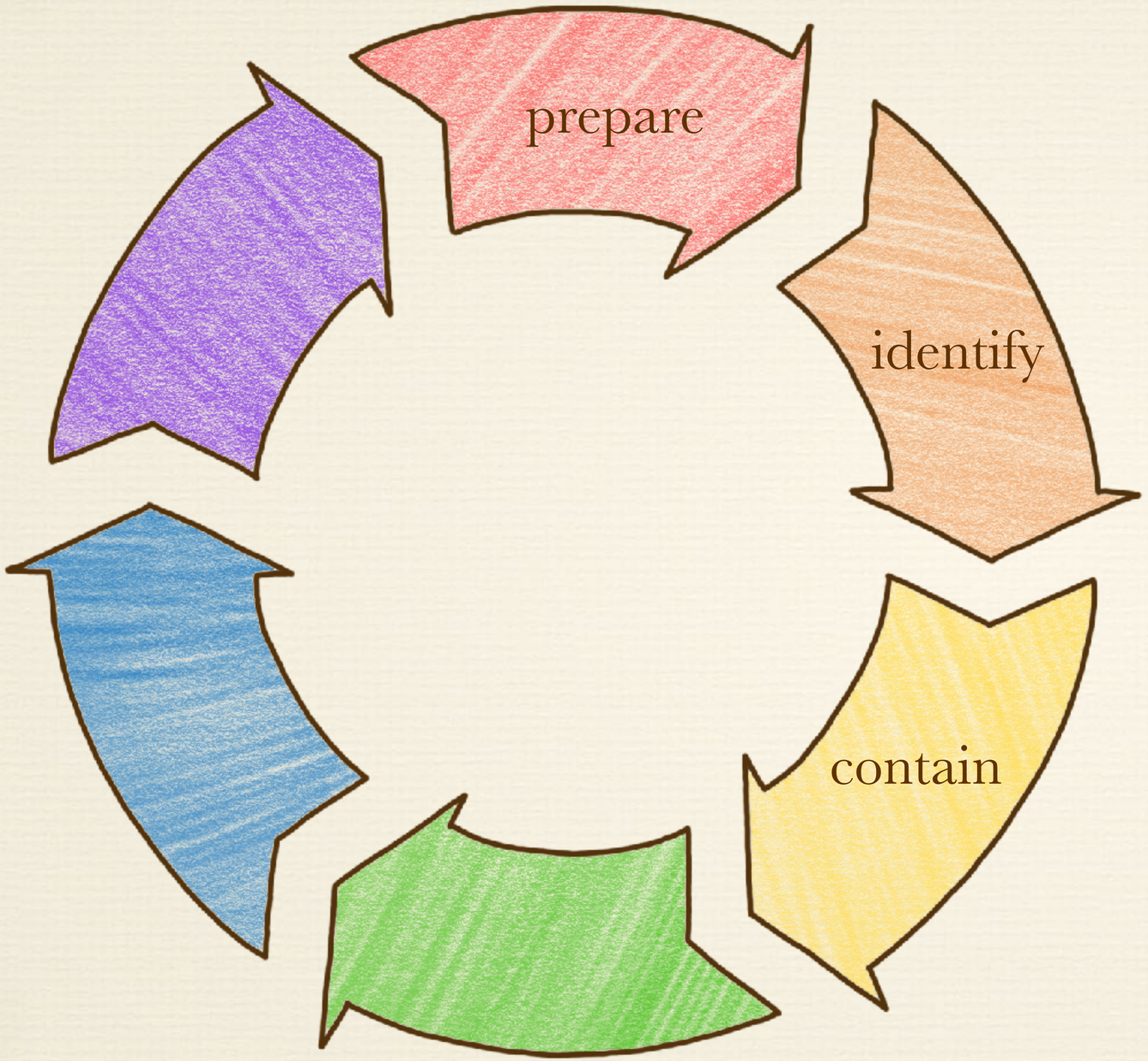
- if you work with at least one other person, you need a plan
- if anyone else uses the systems you look after, you need a plan
- if you've ever forgotten to pack your toothbrush, you need a plan
- if you've ever had a hunch turn out to be wrong, you need a plan
- if you ever get struck by analysis paralysis, you need a plan



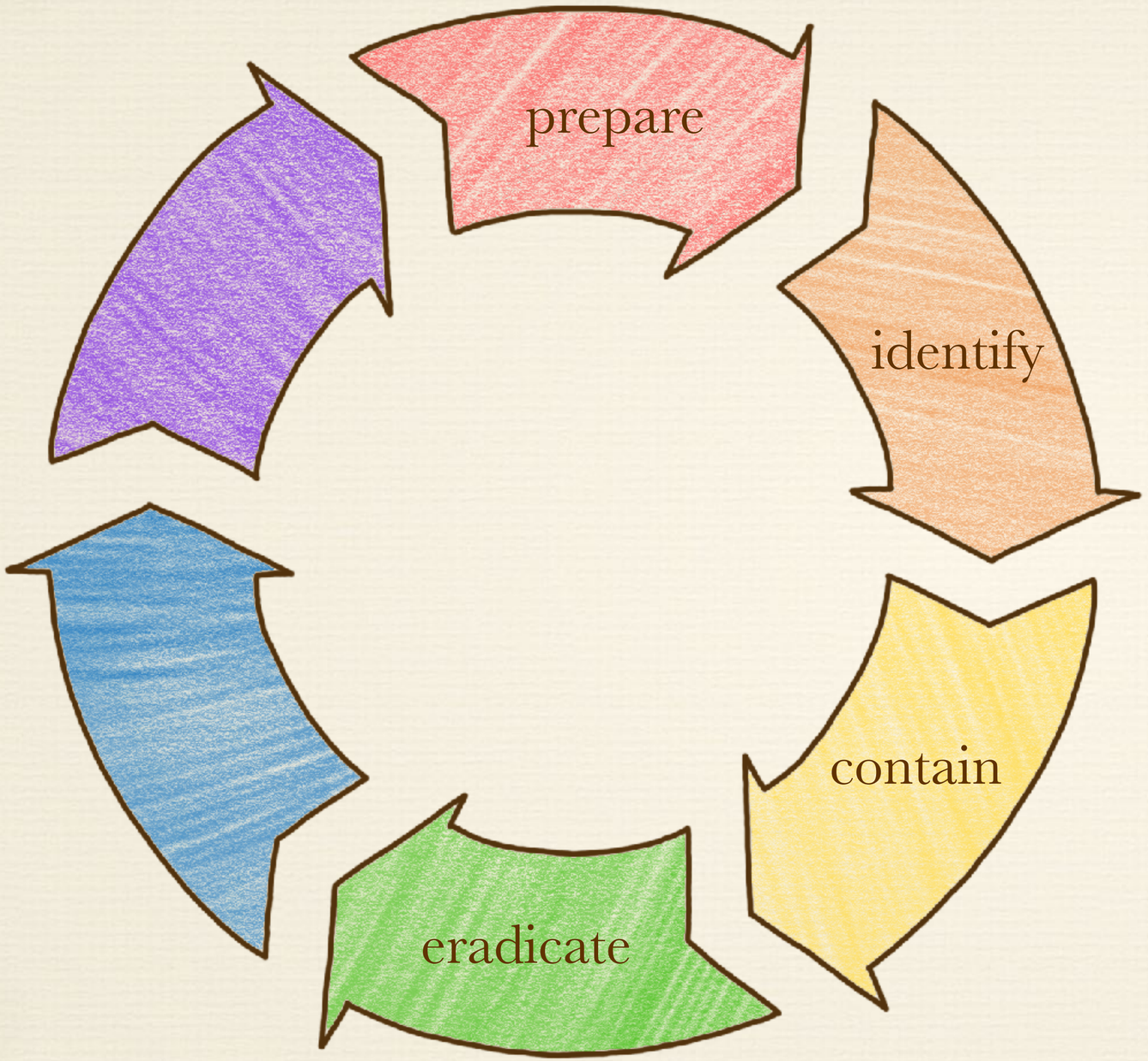
- know what your risks are
- have an incident action plan
- assemble resources you'll need



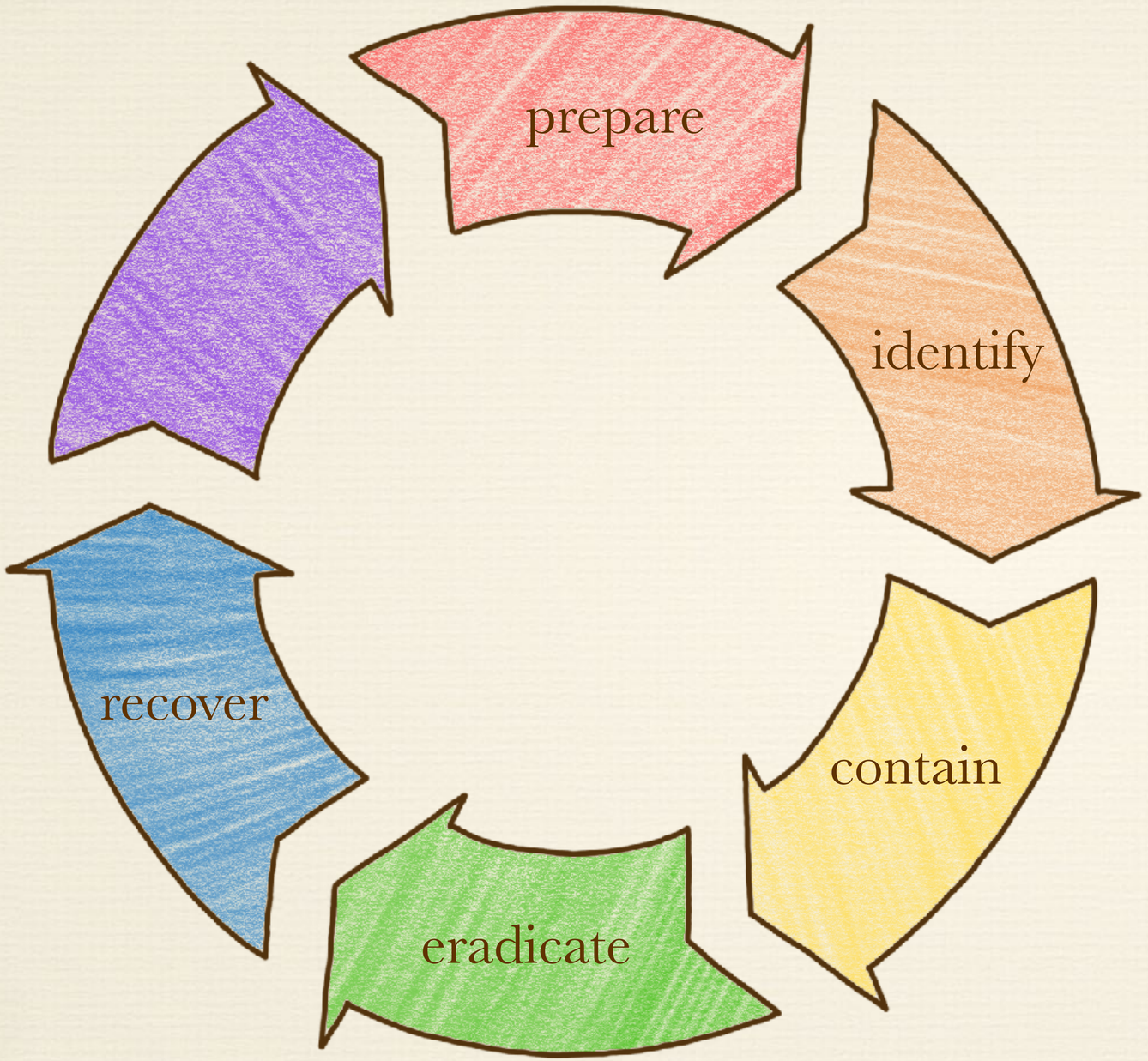
- look out for warning signs
- decide what action to take when a possible incident is discovered
- investigate and gather evidence to understand what happened



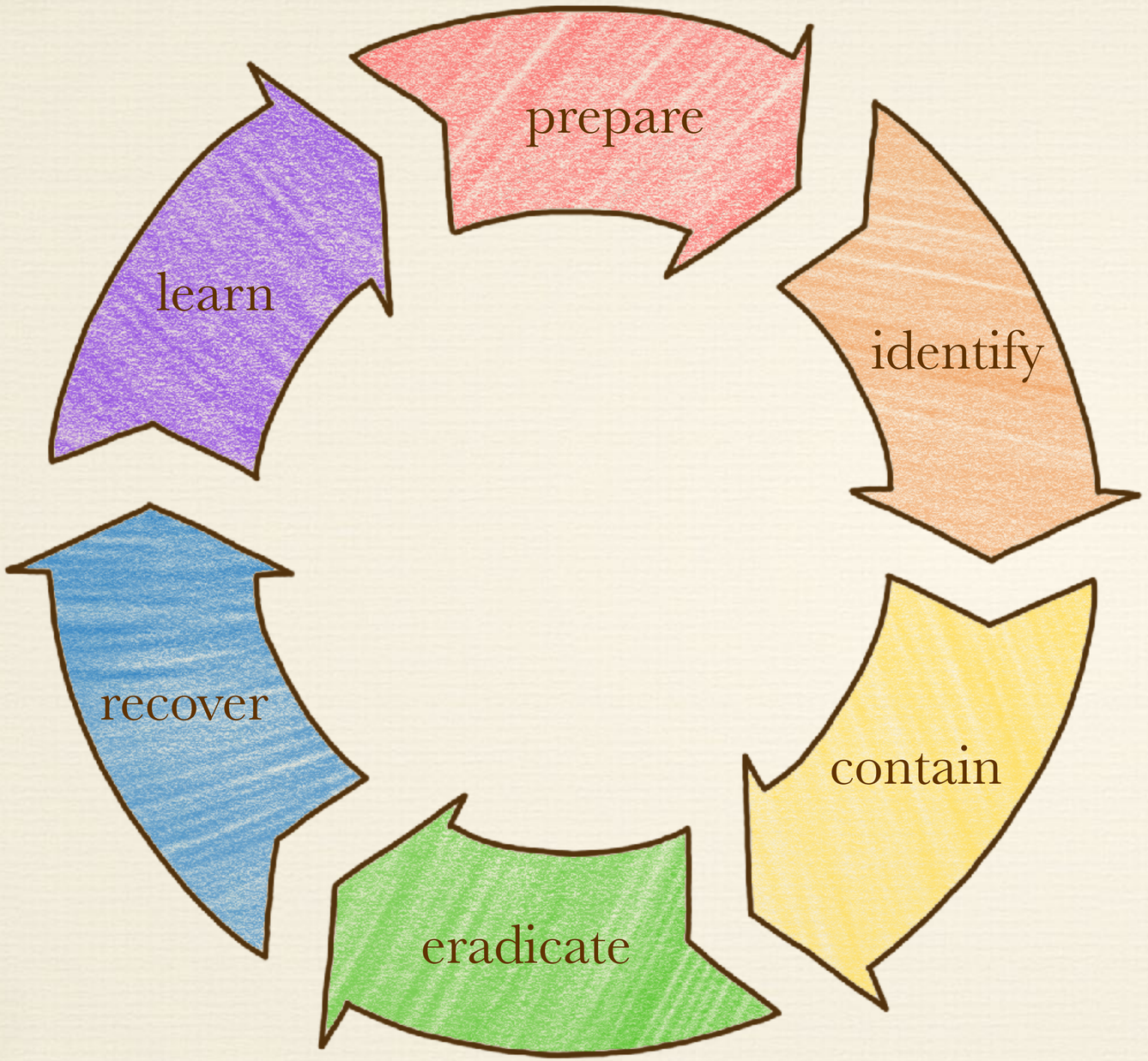
- stop the unwanted activity
- keep the incident from spreading
- manage impact on others



- test and confirm hypotheses
- repair damage caused by incident
- address vulnerabilities that made the incident possible



- get back to business (or vacation)
- confirm that remediations work
- let other people know that the incident has been resolved



- review how the process went
- identify areas for improvement
- make changes for next time

Making an Incident Response Plan is as easy as planning a tropical vacation.

1. Decide who to invite

- Define who will be involved, and what they'll do
- Incident Lead has the power to make executive decisions
- Appoint a Liason/contact for people outside the IR team
- Who will handle customers/clients, media?

2. Do your research

- Understand your threats and risks
- Business continuity objectives
- Contractual requirements / SLAs
- Legal obligations e.g. mandatory privacy breach disclosure

3. Confirm travel arrangements

Work out how you're going to get from A to B – how you'll:

- initiate incident response
- decide you're ready to move from one phase to the next
- declare IR complete

4. Make a packing list

Work out what you need to have in place in order to…

- discover an incident
- communicate and share information
- investigate what happened
- contain, repair and remediate
- restore operations in an acceptable timeframe
- meet any contractual or legal obligations

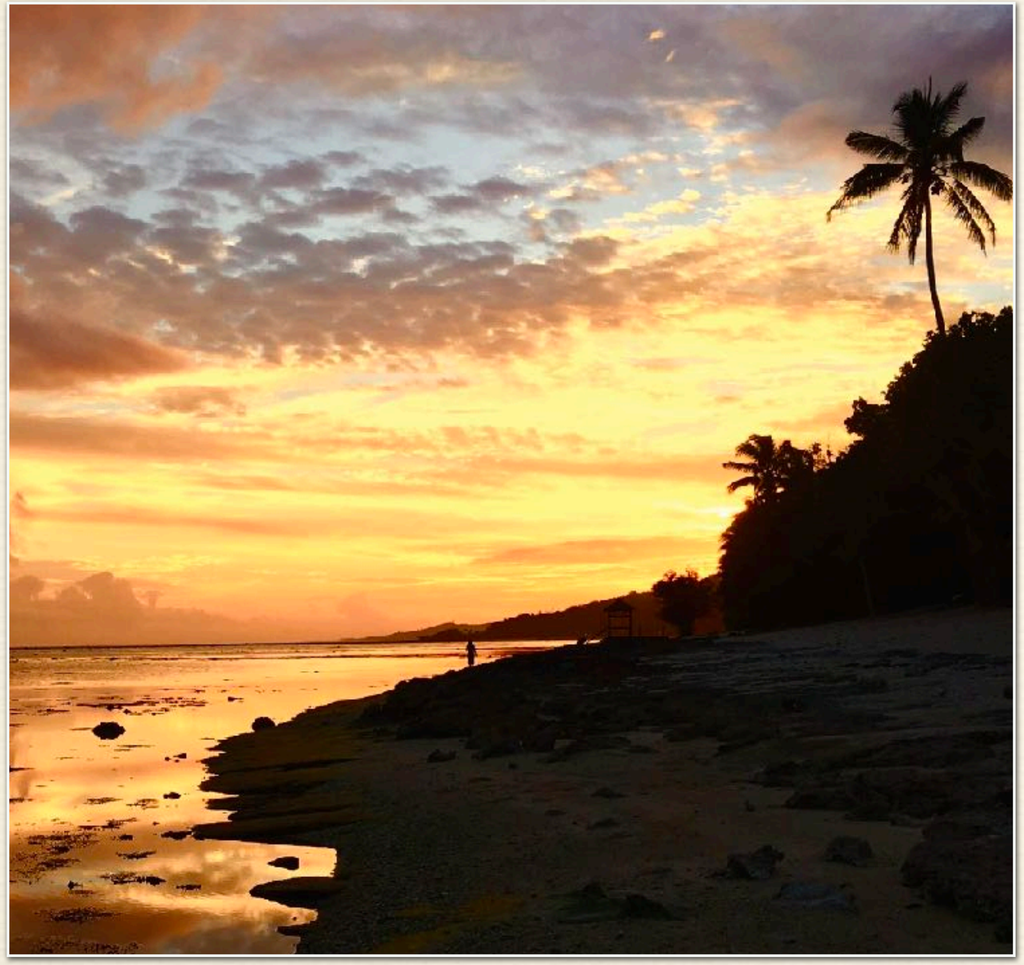
5. Get ready to go

- Make sure everyone is familiar with the plan
- Make sure your pre-requisites are in place and working properly
- Practice – walk-throughs, tabletop exercises and drills
- Review and update the plan regularly

6. Live your best life

- Relax…or go in search of adventure…
- Trust your gut – you've got this!
- Take time to reflect

Summary



- Yes, your team *does* need an incident response plan
- Start small by defining roles, pre-requisites and criteria for moving to the next phase
- Practice the plan often with realistic scenarios
- Always. Be. Catastrophising.