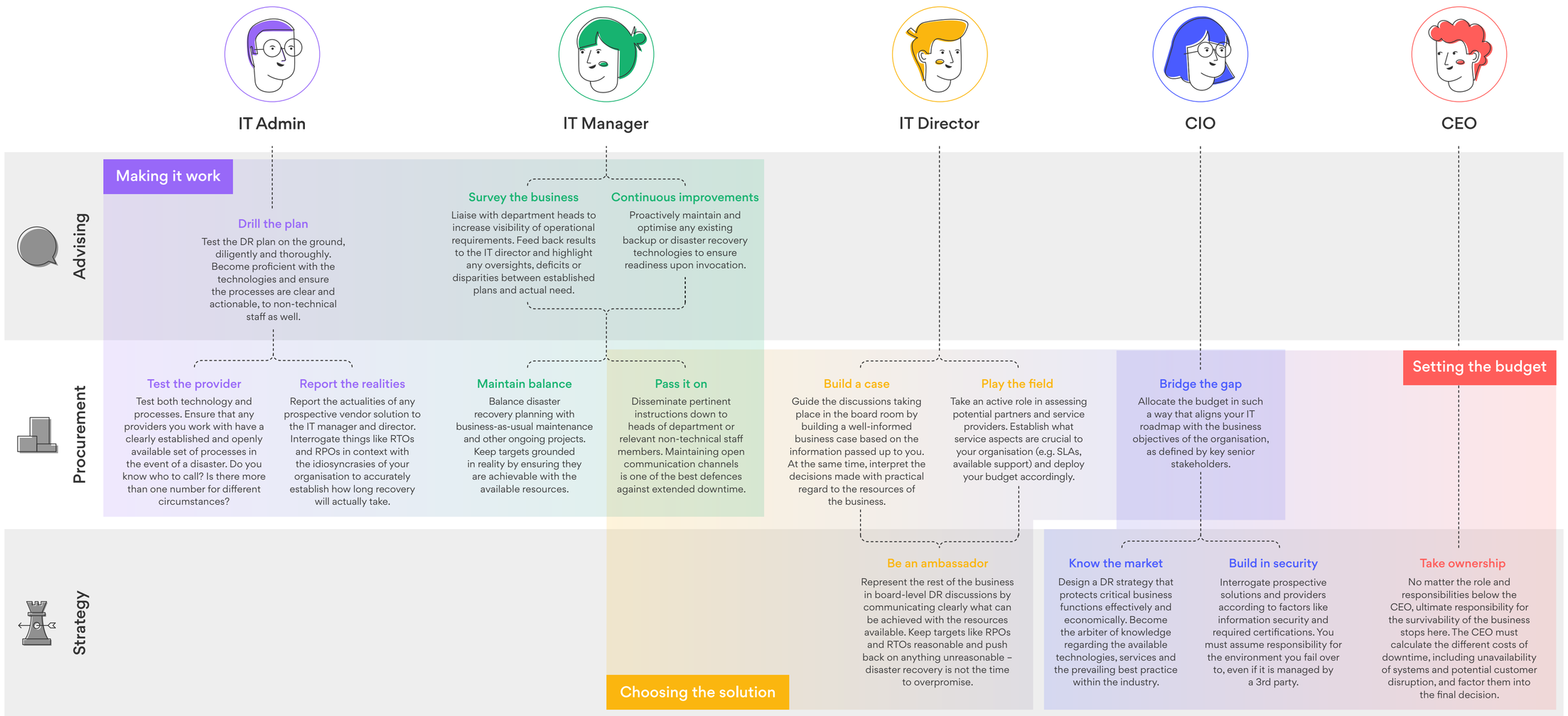
DISASTER RECOVERY RESPONSIBILITIES

WHO IS RESPONSIBLE FOR WHAT IN CREATING A DISASTER RECOVERY PLAN?



WHO IS RESPONSIBLE FOR WHAT IN A DISASTER?

IT Admin

IT admin staff are responsible for the day-to-day running of the systems and services used by the business. Whilst they don't tend to be involved in the design of the BC/DR plan, they usually play a significant role in its execution.

IT Manager

IT managers typically have a broad view of the relationship between the business and the IT it uses. In a disaster, this relates to the technology dependencies between different departments and business functions. Because of this, they often assume a leading role in the coordination of DR processes.

Department Heads

Department heads represent the business units of which the organisation is actually composed. They are responsible for making sure their staff and the systems they use are properly represented in any disaster recovery and business continuity planning.

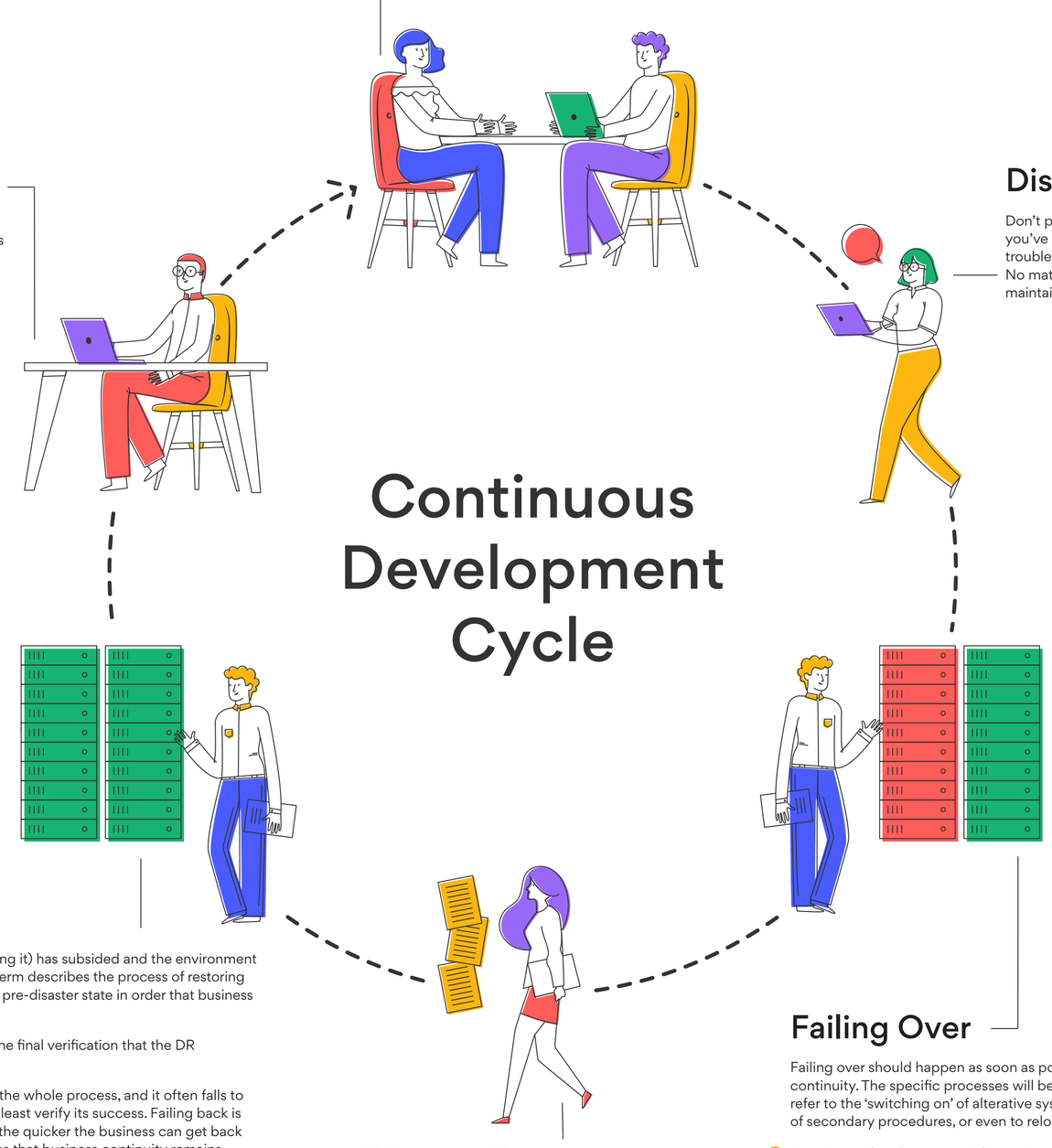
IT Director / CIO

If the IT manager is the figurehead for the practicalities on the ground during a disaster, the director and CIO are the principal representatives for IT among the board. They must pass accurate information to senior stakeholders during disruption regarding what systems and services are affected, how it impacts the business (and its customers), and how long until business-as-usual activities resume.

CEO

The CEO is ultimately responsible for the survivability of the whole business. Rather than assuming any hands-on technical responsibility during a disastrous event, they will instead represent the forward-facing aspects of the company's reputation in any public capacity.

Continuous Development Cycle



Planning

Though at first planning precedes disaster, it's also an ongoing activity that never really stops. DR and business continuity plans should be continually reviewed and updated (particularly after any significant business change) to keep them in line with current business needs.

- Senior stakeholders hold ultimate responsibility for the business. They must prioritise DR/BC planning and actively establish what departments and IT functions are critical to the business. This includes high-level decision making and budget allocation, as well as in-depth analysis (and continual review) of recovery requirements on a per-department basis.
- Technical operational staff must contribute to planning by passing accurate information about different departmental needs up the chain of command. If this communication breaks down, the decisions made in the board room will not reflect the realities on the ground.

Disaster!

Don't panic! If you've planned well, you've already done the hard work. Just troubleshoot, firefight and prepare to invoke. No matter the scale of disruption, focus on maintaining clear communication channels.

Failing Over

Failing over should happen as soon as possible to minimise disruption to business continuity. The specific processes will be different for every organisation: it might refer to the 'switching on' of alterative systems and resources, or to the invocation of secondary procedures, or even to relocating to a secondary office space.

- Department heads represent the portion of the business DR plans are designed to protect. They often take an ambassadorial role in communicating how the disaster (and recovery) is experienced on the ground, both as its happening and during review.
- IT admin staff are often the bridge between the user experience and the technical controls within the DR plan. Their job is to execute the instructions laid out in the plan and to interpret feedback from department heads into further actionable steps.
- IT managers are the lynchpin of disaster events; whether the DR plan is executed in-house, or in partnership with a 3rd party provider, all communications should travel through them. Resources must be allocated evenly between diagnostic and repair work, and invocating the agreed-upon failover steps. Though CIOs and CEOs are ultimately responsible for ensuring the DR plan can save the business, the IT manager is responsible for ensuring that it does.

Disaster Resolved

The degree to which failing back becomes urgent depends on the business-as-usual functionality your DR plan permits. If only business-critical functions are restored, the pressure to fail back as soon as possible increases. DR plans with a more comprehensive remit may enable the business to work more productively, for longer.

Failing Back

Once the disaster (and the conditions causing it) has subsided and the environment stabilised, the business must fail back. The term describes the process of restoring affected IT systems and procedures to their pre-disaster state in order that business as usual activities can resume unimpeded.

- As with failing over, department heads are the final verification that the DR controls achieve their intended results.
- Failing back is the most important stage in the whole process, and it often falls to the IT admins to execute the plan, or at the least verify its success. Failing back is arguably more important than failing over; the quicker the business can get back to business as usual, the greater the chances that business continuity remains uninterrupted.
- Failing back ultimately depends on fault resolution, and it falls to the IT manager to coordinate this process. Once the cause of the failure has been established and steps taken to rectify the issue, the IT manager must oversee the restoration of business-as-usual systems.

Review

There's no better time to review your DR/BC plans than in the wake of a disaster. This isn't your standard annual review; it's an opportunity to extract real value and intelligence from major disruption. Once review processes are concluded, the results can be built into future planning processes to improve future resilience.

0800 033 6633
contact@databarracks.com
www.databarracks.com

Databarracks
1 Bridges Court
London, SW11 3BB

Databarracks