Assessing disaster recovery programme maturity: A practical approach

Received (in revised form): 12th May, 2023

Kevin Finch

Senior Business Continuity Architect, Sayers, USA

Kevin Finch *has been a business continuity and disaster recovery practitioner for the past 17 years, after working for a decade in client-server application support. He has built business continuity programmes from the ground up in financial services, insurance, logistics and auto manufacturing companies, and been a speaker at numerous business continuity and information security conferences. Kevin has also been a member of* Disaster Recovery Journal*'s glossary committee since 2017.*

Abstract

The process of measuring the overall maturity of a disaster recovery programme can be accomplished by measuring the maturity of the individual processes that make up the programme, and then looking at the results in aggregate. For each process, two aspects require particular attention: the maturity of the process itself, and the extent to which the process is utilised through the organisation as a whole. This paper discusses the process of measuring process maturity, and outlines a practical methodology for applying that process to the appraisal of disaster recovery programmes. It discusses the importance of looking at how widespread different disaster recovery processes are in the business, and outlines a practical approach to conducting programme appraisals.

Keywords: disaster recovery, maturity, assessment, metrics, measurement, programme improvement

MEASURING PROCESS MATURITY

I consider this article to be a practical guide rather than a scholarly work on measuring process maturity, because I do not consider myself an expert in the field. There are various methods for measuring process maturity, and this article will not be examining multiple methods or discussing the virtues of one method over another. However, in order to understand the maturity measurements that we are planning on using, we need to have some basic knowledge of what process maturity is and how it is measured.

To measure the processes and therefore overall programme maturity, this article uses an adapted version of the capability maturity model integration (CMMI). The CMMI was developed in succession to the original capability and maturity model (CMM). The CMM itself was developed between 1987 and 1997 to help measure the maturity of software development programs;[1] the CMMI came out afterwards as a way to, among other things, adapt the model to cover agile software development. The model has since gone through multiple iterations to adapt to the changing landscape of the software development industry. The CMMI looks at the predictable evolution of business processes as they improve, and provides a methodology for quantifying the state of process maturity based on that state of evolution. The CMMI can accomplish this because there is a predictable sameness to the way

Kevin Finch

Sayers,
960 Woodlands Parkway,
Vernon Hills, IL 60061,
USA

Tel: +1 615 686 3347;
E-mail: kfinch@sayers.com

Journal of Business Continuity & Emergency Planning
Vol. 17, No. 1, pp. 31–38

1749–9216

business processes tend to evolve as they mature as regards governance, documentation and performance metrics.[2]

In general terms, as business processes develop and mature, they usually follow the same pattern. Processes tend to start out as disorganised groups of tasks performed on an *ad hoc* basis. Then, as time goes on, the processes tend to become documented for consistency and those processes tend to begin to be assigned to staff that take over some share of responsibility for them. Eventually those processes get to the point that they are defined at an enterprise level — they are completely documented, ownership for the processes is defined, procedures are standardised and the process documentation is widely available. If the process continues to mature, then metrics will start to be used to measure the health of the process so that the quality of service (and the risk it represents to the organisation) can be measured, documented and improved, and the process itself is capable of being scrutinised or even audited. If the process matures beyond that point, then eventually the process will be governed proactively instead of reactively, often shifting to a posture of continuous improvement rather than simply monitoring and maintaining the status quo.

Corresponding to each of these states, the CMMI scale has five incremental stages of increasing process maturity.

As Figure 1 illustrates, Stage 1 is that initial stage where work is disorganised and carried out on an *ad hoc* basis. Then, as the process becomes more established, documented and repeatable, it will eventually evolve into Stage 2 of maturity. Once it is completely defined and documented, and ownership is better defined, it evolves into Stage 3 of maturity. If it evolves to the point where process health is being monitored and key metrics are established to control the process, the process has evolved to Stage 4. If it continues to evolve past that point so that the process is not only being tracked but continually monitored and improved, then it has evolved to Stage 5.

That, at least, is the theory. It is important to note that many (if not most) business processes never get much beyond Stage 3 (in my experience). Once a process is completely documented and centrally managed, then that is 'good enough' for a lot of companies; they might see increases in the quality of service or efficiency of operations if they started monitoring a process proactively and tracking metrics, but they might not find that to be practical or realistic.

For a real-world example of process maturity beyond the theoretical, consider an example that nearly everyone has encountered at least once in their lives: submitting a ticket to the IT helpdesk. Anyone who has ever tried to open a ticket at a small company will probably have experienced a ticketing process that was a little disorganised and a response process that may have been somewhat informal (Stage 1). At a bigger company, there may have been an actual helpdesk you called instead of a single person, and the process was more formalised and consistent (Stage 2). If the company was bigger still, then that process would probably be even more consistent. There might be formalised processes that were well documented for specific service requests, like restoring a file or setting up a new user, and the helpdesk organisation had a clearly defined owner (Stage 3). A more mature helpdesk might start looking at metrics to improve customer service, like the time to resolution for tickets, and they would be providing those metrics to their management to help govern decision-making on things like staffing (Stage 4). If you have dealt with a large, world-class company's helpdesk, you may have seen processes that have evolved beyond even that. They may be using self-service processes to minimise the time and effort to get help, and they may even send out feedback surveys to see

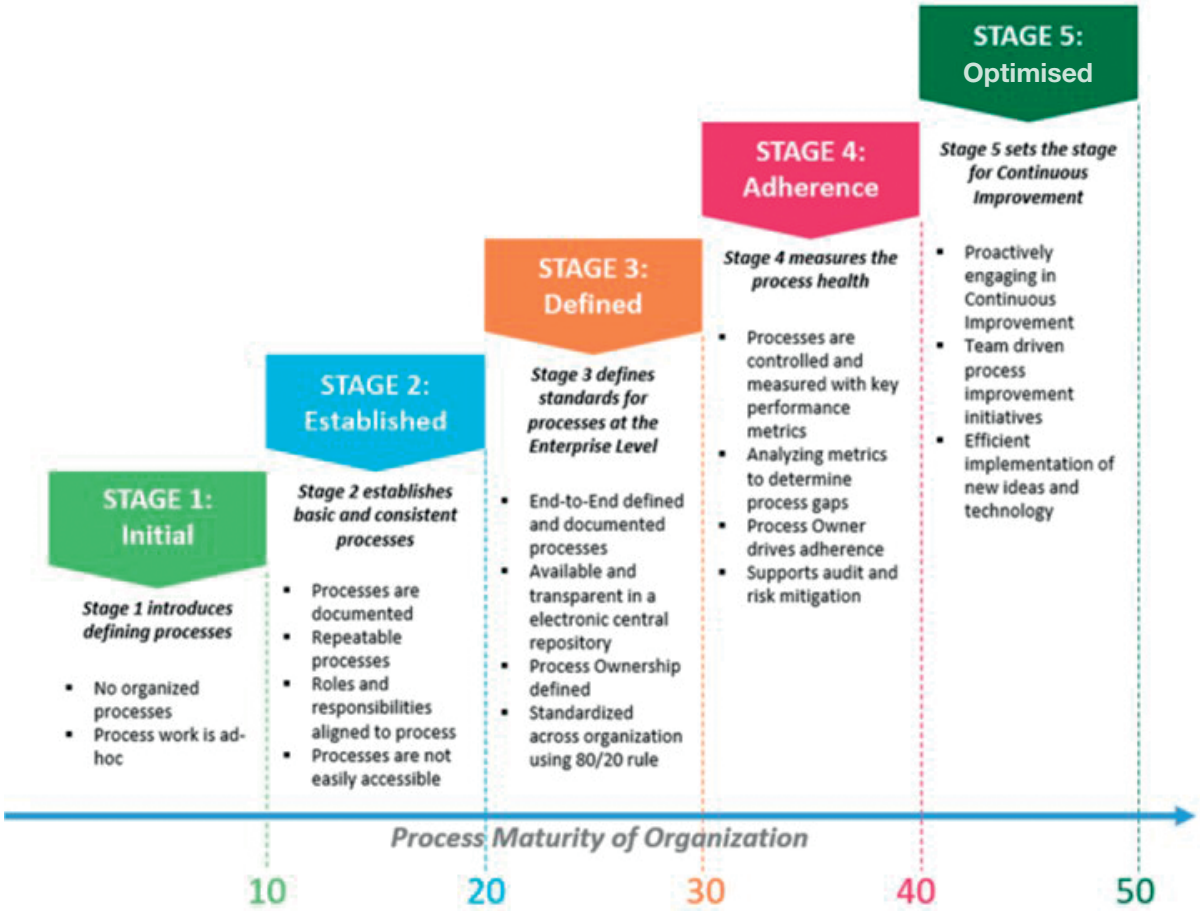

Figure 1 The five stages of process maturity

Source: Berkeley Process Management Group, University of California, Berkeley (n.d.) 'Process Maturity', available at https://bpm.berkeley.edu/process-architecture/process-maturity (accessed 7th April, 2023). Reproduced with permission.

how they can continue to improve their service (Stage 5).

Thinking through this example (and my own experiences), it is easy to see why a lot of processes never make it past Stage 3 of maturity. If a company has developed a formal, centrally managed process that is well documented, then that probably does everything they need. They may feel there is not a lot of incentive for them to mature the process beyond that.

Best practices also come into play to some extent, and there are parallels between many sets of best practices and overall process maturity. However, there are often multiple sets of best practices pertinent to a given business process, so some research might be required in picking the one that best suits your environment. Thinking back to the helpdesk example, the Help Desk Institute,[3] Information Technology Infrastructure Library,[4] Service Desk Institute[5] and the International Association of IT Asset Managers[6] have all published best practice guidelines for running a helpdesk. While those sets of best practices are largely complementary to each other, each is unique from the others in areas of emphasis.

It is also worth noting that, while there are often parallels between best practices and process maturity, a strict adherence to best practices may not always be what

matures the process. Likewise (and perhaps more importantly) maturing a process does not always bring it more into alignment with best practices. It is entirely possible to have a continuously monitored, self-improving, Stage 5 maturity process that goes against best practices.

If we want to classify a process and determine where its maturity fits into the CMMI model, we do what is known as an *appraisal*. At the risk of oversimplifying the process, a CMMI-style appraisal effectively works as follows:

- The areas of interest for the appraisal are selected (NB: practice areas can vary by organisation);
- A set of best practices to be followed is also selected;
- Practice areas are evaluated individually for how closely they adhere to the appropriate best practices and where they are along the CMMI maturity continuum;
- Scores are created and tabulated based on those evaluations.

MEASURING DISASTER RECOVERY PROGRAMME MATURITY

Appraising a disaster recovery programme differs from the basic appraisal approach outlined previously as, before all else, we need to refer to best practices for guidance on which practice areas to appraise. This approach tends to hold true in the existing maturity modelling processes in the resilience space as well. It does not matter if the company is using disaster recovery best practices from the Disaster Recovery Institute International (DRI), the International Organisation for Standardisation (ISO) and their ISO 22301 or ISO 27001 standards, National Institute of Standards and Technology, the Information Technology Infrastructure Library or the US Federal Emergency Management Agency. Whatever best practices the company has chosen to follow should determine which practice areas of its disaster recovery programme to appraise for maturity.

For this example, we will use the best practices guidance put together by the DRI. According to the DRI, there are ten broad areas of practice[7] that need to be covered when implementing and maintaining a disaster recovery programme. These can be grouped into the following areas:

- *Defining*: Define the requirements for the disaster recovery programme;
- *Implementing*: Create the disaster recovery programme documentation and implement the disaster recovery solution;
- *Maintaining*: Establish a process to validate, review and update the disaster recovery programme and its components.

Underneath these practice areas, we should break things down further in order to look at the performance of individual areas. For example, we would want to break down defining the programme requirements into asset management, risk management and performing a business impact analysis (BIA), as these all contribute to defining the scope of the organisation's disaster recovery programme. Risk management could in turn be broken down into appraising internal and external risks, while asset management could be further broken down into hardware asset management, software asset management and system configuration management, each of which represents an important piece of the whole and may have its own set of independent processes that need to be followed. The BIA process could also be broken down to look at system recovery tiers and whether

recovery time objectives (RTOs) and recovery point objectives (RPOs) have been assigned. Or, to put this example into an outline form:

(1) Defining the disaster recovery programme:
    (a) Asset management
        (i) Hardware asset management
        (ii) Software asset management
        (iii) System configuration management
    (b) Risk management and mitigation
    (c) Performing a BIA
        (i) System recovery prioritisation
        (ii) Assignment of system/application RTOs
        (iii) Assignment of system/application RPOs

The entire programme will need to be broken down in this manner so we can appraise the maturity of each part in isolation. Therefore, in this example, we would be looking at eight separate programme components to appraise to assess the maturity of the overall disaster recovery programme definition.

With this list of programme components compiled, then we move on to assessing the programme's maturity. For this, we would go through each component and appraise where it lands in the CMMI continuum, looking at the specific characteristics of that work effort to determine the highest maturity stage that is fully completed. Using RTOs as an example, we might be looking at something like this to determine the stage of maturity:

- *Stage 0*: No RTOs assigned;
- *Stage 1*: *Ad hoc* assignment of RTOs;
- *Stage 2:* Informal RTO assignment (ie not based on a standard impact analysis);
- *Stage 3*: RTO assignment is based on a standardised impact analysis, documented, and approved by business leaders;
- *Stage 4*: RTO assignment is based on a standardised, comprehensive quantitative and qualitative impact analysis;
- *Stage 5:* RTOs are reviewed, updated, and approved as required (eg as part of change management) as well as during annual reviews.

In the previous programme definition example, we would be doing this CMMI stage assessment eight times, as there are eight separate programme components, so this is not particularly labour-intensive. With those criteria set for all of the components of the programme, we are able to assess the overall maturity. We assess the maturity stage of each individual part and then we can aggregate the results of those assessments to determine the maturity of the programme as a whole. Once the programme components are listed out, the assessment itself can be completed in a few hours. For a more in-depth assessment, the programme components can be broken down further, and the underlying processes can be examined at a more granular level.

COMPLETION STATUS

The completion of disaster recovery programme components also needs to be examined to determine the overall maturity of the programme. In this case 'completion' refers to the extent to which the programme component is being deployed across the entire enterprise. If a process is mature, but not widely used, then its actual utility in helping to recover the enterprise is limited.

This is why, in addition to a CMMI stage appraisal, the appraisal really should include a completion status assessment of the various programme components. Your enterprise might need a higher level of

granularity, but I have found that breaking down the completion percentage into groups allows for a sufficient level of accuracy and speeds up the assessment process. (It is hard to come up with an exact completion percentage, but it is generally pretty easy to come up with a ballpark estimate.)

Using the example of RTOs from earlier, let us say that we are sitting at Stage 5 for the maturity of the RTO process. The RTOs are calculated from a completed BIA, they are being reviewed, updated and approved annually, and they are also getting revised as needed whenever there is some change in the environment that could affect them. However, if we have only got RTOs assigned to about 40 per cent of the applications and/or systems in the environment, then that high level of maturity is not going to translate into a high level of preparedness for the company overall, as regards RTOs. A breakdown of RTO completion statuses might look something like this:

- *Level 0*: No RTOs assigned;
- *Level 1*: 1–25 per cent of applications/systems have RTOs assigned, and this is documented (eg in a tool or spreadsheet);
- *Level 2*: 26–50 per cent of applications/systems have RTOs assigned, and this is documented;
- *Level 3*: 51–75 per cent of applications/systems have RTOs assigned, and this is documented;
- *Level 4*: 76–99 per cent of applications/systems have RTOs assigned, and this is documented;
- *Level 5*: 100 per cent of applications/systems have RTOs assigned, and this is documented.

It is also worth noting that 100 per cent completion has its own category. There is usually a high level of effort required to get from 'about 99 per cent' to a 'documented 100 per cent complete' for any of these programme components, and that extra effort is worth noting. It is also important to strive for 100 per cent completion in all aspects of the disaster recovery programme, even if the process maturity is not very high. In an actual disaster recovery incident, a business is probably better off with high completion percentage and a lower maturity, than they are with a high maturity and low completion percentage.

BRINGING IT ALL TOGETHER

Once completed, a spider diagram is helpful for presenting results. Figure 2 provides an example of what Sayers uses when presenting this information to a client following an appraisal.

In summary, to assess the maturity of a disaster recovery programme:

- Choose the set of disaster recovery programme management best practices that best suits your business;
- Break down those best practices into specific programme components that can be individually evaluated;
- Evaluate the CMMI maturity stage of each one of those programme components, based on the way the process is currently being performed; and
- Evaluate the completion percentage of each of those programme components, scoring them on how widely they are currently being used across the enterprise.

Once the data have been collected and tabulated:

- Go through the programme component maturity stage scores with management and determine which components need attention. For many components,

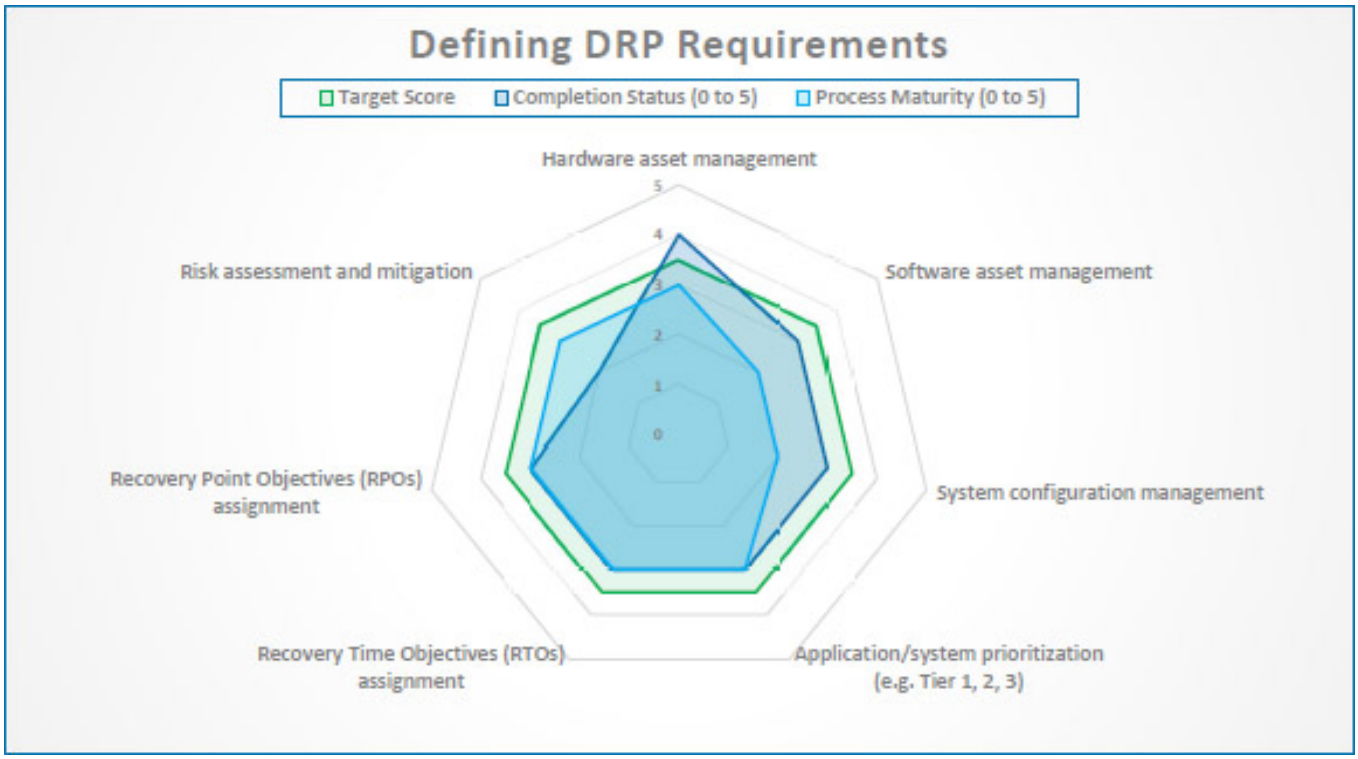

Figure 2 Defining disaster recovery programme requirements

Source: Sayers (2023) 'DR Maturity Assessment Results (Sample)_v3'

a Stage 3 or Stage 4 might be all you need, but any Stage 1 or 2 components probably need attention;
- Look at the completion scores and see what areas need attention;
- See if there are any programme components where efforts to improve them could be combined. For example, an effort to increase completion of RTO scoring could easily be combined with finishing a BIA and trying to complete RPO scoring. Likewise, it would make sense to try and increase the completion of your hardware asset data at the same time you completed your software asset data and filled out your configuration management database;
- Come up with a complete list of all the areas that need attention and prioritise it;
- Develop a plan for the next 18 months and also a three-year plan, to get all of the issues addressed;
- Repeat the assessment process every 9–12 months to track progress.

By the time your business has worked through that three-year plan, you will be much better prepared and have a much more mature and resilient disaster recovery programme than you had at the start.

References

(1) Wikipedia (2022) 'Capability maturity model integration', available at: https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration (accessed 7th April, 2023).
(2) University of California, Berkeley (n.d.) 'Process Maturity. Berkeley Process Management Group', available at: https://bpm.berkeley.edu/

process-architecture/process-maturity (accessed 7th April, 2023).
(3) Help Desk Institute (n.d.) 'About HDI', available at: https://www.thinkhdi.com/about.aspx (accessed 7th April, 2023).
(4) IBM (n.d.) 'IT infrastructure library (ITIL)', available at: https://www.ibm.com/topics/it-infrastructure-library (accessed 7th April, 2023).
(5) Service Desk Institute (n.d.) 'About SDI', available at: https://www.servicedeskinstitute.com/about-sdi/ (accessed 7th April, 2023).
(6) International Association of IT Asset Managers (n.d.) 'About us', available at: https://iaitam.org/about-us/ (accessed 7th April, 2023).
(7) Disaster Recovery Institute International (2017) 'Professional Practices for Business Continuity Management', available at: https://drii.org/resources/professionalpractices/EN (accessed 7th April, 2023).