

# The State of Change Management

Why change management is failing in many organisations

---

Karen Ferris, Macanta Consulting

## ABSTRACT

Forrester research (2011) revealed the poor state of change management in the majority of organisations surveyed. This paper explores the reasons that change management is failing in so many organisations and the actions that need to be taken to rectify the situation.

**TABLE OF CONTENTS**

<b>1</b>	<b>Executive Overview .....</b>	<b>3</b>
<b>2</b>	<b>Introduction .....</b>	<b>4</b>
<b>3</b>	<b>Why Change Management is Failing .....</b>	<b>5</b>
3.1	The Lifecycle.....	5
3.2	Project Management and the Change Schedule .....	6
3.3	Education, Awareness and Continual Improvement .....	7
3.4	Zero Tolerance and Organisational Culture .....	7
3.5	Management Commitment.....	9
3.6	The CAB .....	9
3.7	The ECAB .....	10
3.8	Risk Assessment .....	11
3.9	Monitor, Measure and Act .....	12
3.10	Accountability .....	12
3.11	Streamline.....	13
3.12	Service Asset and Configuration Management .....	14
3.13	Service Provider Groups.....	14
3.14	Technology Exploitation .....	14
<b>4</b>	<b>Conclusion.....</b>	<b>15</b>

## 1 EXECUTIVE OVERVIEW

Forrester research has revealed that change management in the majority of organisations is not working as intended. An unacceptable number of incidents are the result of changes being made to infrastructure, applications, processes or tools.

In today's world where applications are more stable and infrastructure is more resilient, the number of incidents relating to their failure should be minimal. Therefore the incidents relating to their failure are most likely because someone has changed something and caused it to fail.

Change management as a process has been around since the earliest days of ITIL®<sup>1</sup> and despite being improved and developed over the years, the basics are still the same. Therefore why is change management not having the desired effect of controlling changes and ensuring that there is minimal impact on the delivery of service to our customers?

This paper explores some of the reasons that change management is failing in so many organisations and proposes actions that can be taken to rectify the situation.

These include failure to implement the change management process across the entire service lifecycle and instead implement it as an operational gateway; a disconnect between changes and projects; lack of education and awareness about the process; lack of policies regarding non-adherence to process and acceptance of undesired behaviour; inflexibility and bureaucracy of the Change Advisory Boards; lack of measurement and actions taken to bring about improvement; failure to continually streamline the process and failure to take advantage of available technologies.

---

<sup>1</sup> ITIL® is a Registered Trademark and A Registered Community Trademark of the UK Cabinet Office in the United Kingdom and other countries.

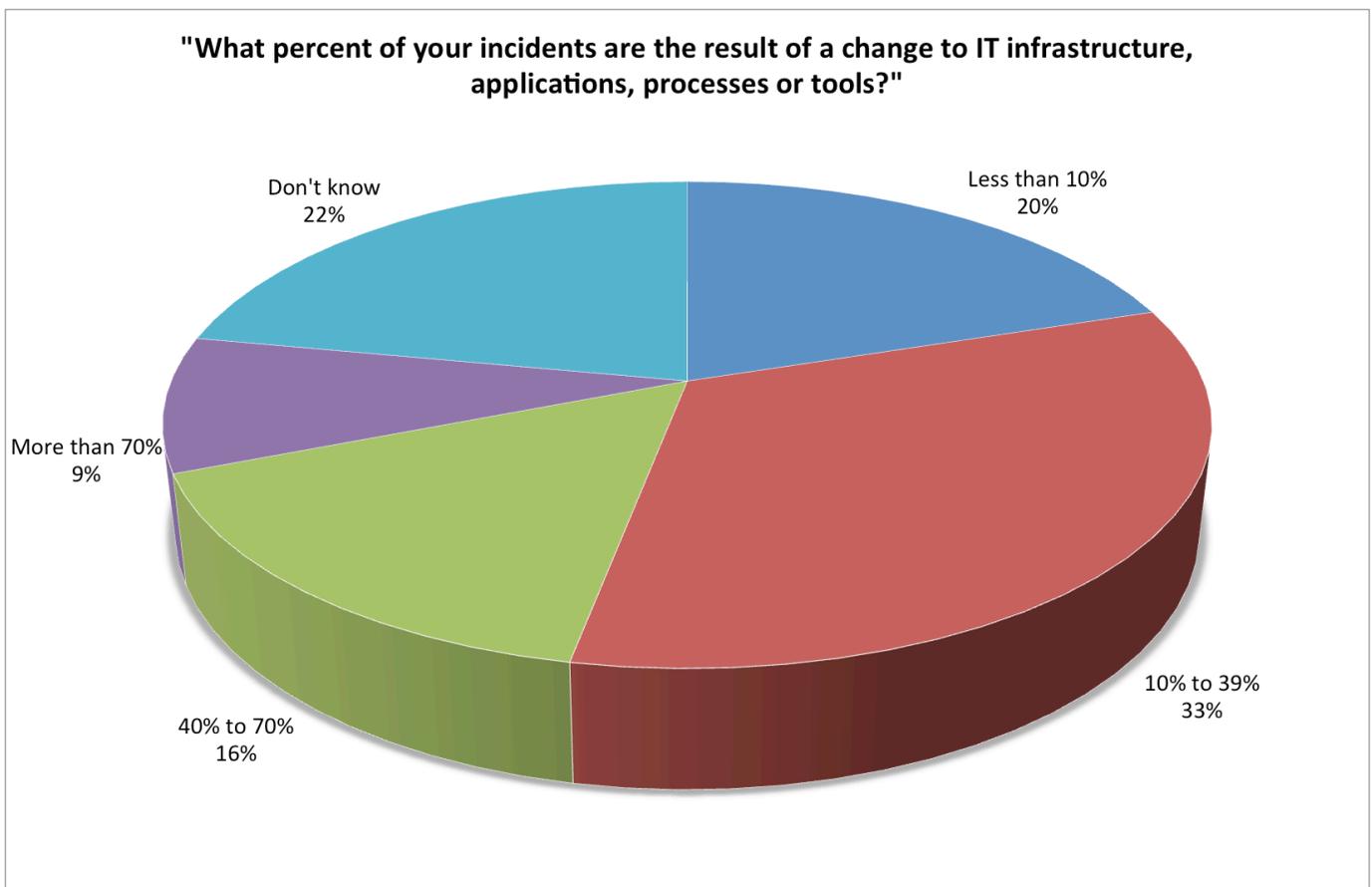
## 2 INTRODUCTION

In November 2011, Forrester issued a report entitled the "The State of IT Service Management in 2011"<sup>2</sup>. In conjunction with itSMF USA<sup>3</sup>, Forrester surveyed 491 IT Service Management (ITSM) professionals and the report of the results by Glenn O'Donnell contains many interesting insights, including one concerning change management.

Although 95% of the survey respondents were from North America, my experience in Australia and elsewhere leads me to believe that the findings would be consistent with the state of change management in other countries.

The survey asked, "What percent of your incidents are the result of a change to IT infrastructure, applications, processes or tools?"

The following graph shows the results.



Source: Forrester / itSMF Q2 2011 US ITSM Online Survey

20% of respondents indicated that less than 10% of their incidents were the result of these types of changes. Although not a perfect score (which would be zero) this is a good result for 1/5 of the survey group.

<sup>2</sup> [http://www.forrester.com/rb/Research/state\\_of\\_it\\_service\\_management\\_in\\_2011/q/id/60866/t/2](http://www.forrester.com/rb/Research/state_of_it_service_management_in_2011/q/id/60866/t/2)

<sup>3</sup> <http://www.itSMfusa.org/>

Over half of the respondents (58%) are operating in unacceptable environments and nearly a quarter just don't know! The latter is the most worrying of all the results.

Change management is a process that has been around since the earliest days of ITIL. It has been developed and improved over the years, but the basic principles haven't really changed that much. So why is the state of change management in such disarray?

### 3 WHY CHANGE MANAGEMENT IS FAILING

Why is the process failing to meet its purpose as stated in ITIL?

*The purpose of the change management process is to control the lifecycle of changes, enabling beneficial changes to be made with minimum disruption to IT services. ITIL Service Transition, Cabinet Office, 2011*

This paper will discuss why change management is failing in so many organisations. It is not the intent of this paper to document the change management process itself. The reader can refer to ITIL and other sources of best practice to determine what the change management process should look like. The intent of this paper is to highlight the aspects of the process that are causing it to fail and propose actions that can be taken to rectify the situation.

#### 3.1 The Lifecycle

The first answer is in the definition above. The purpose of the change management process is to control the lifecycle of changes. In many organisations change management has been implemented as an operational change control mechanism. That is as a gate into the production environment and not as a lifecycle process.

The so-called change management process is initiated when a change is ready to be moved into operational use. All the design, build and testing has been completed and the change now needs to be placed into the production environment.

The intent was that the change process should be initiated when the need for a change is first identified. This could be from service portfolio management, incident management, problem management, request fulfilment or any other service management process.

Once the need for a change is identified a request for change (RFC) should be raised for assessment by key stakeholders i.e. the Change Advisory Board (CAB). (Note however that some changes are pre-approved or pre-authorised by the CAB so assessment is deemed to have been performed already).

The RFC then undergoes an assessment of risk, business continuity, change impact, resource requirements, return on investment, value on investment, scheduling conflicts etc. The RFC is in fact a change proposal that is submitted before any design, build or testing has taken place. If following the assessment, there is approval for the change to proceed, the change then enters the design phase. Depending on the nature of the change, it may become a project but should still fall under the scope of the change management process.

RFCs that are approved will become change records in which the details of the change are recorded during its lifecycle. The change will be subject to a number of

assessments during its lifecycle, depending on the nature of the change. Once design is considered complete the change may be reassessed to determine whether it is ready to enter the build phase. Once build is complete, the change may be reassessed to determine whether it is ready to transition into testing and once testing is complete the change will be assessed to determine whether it is ready to be moved into operational use.

When change management is implemented as an operational gate only and all the design, build and test has already been completed, the value of the assessment for operational use is largely diminished. At this point even if the assessment considers the change not suitable for operational use the chances of the change being "rejected" is minimal as all the investment has already been made. The money has been spent! The pressure will be on to put the change into production regardless of the impact it may have.

The other consequence I often see when change management is just an operational gate is that the project team or change implementer is faced with an unforeseen hurdle when trying to move their change into the production environment. All the pre-work has been done, the implementation date agreed with the business and then they are faced with a change management process that is asking questions about the change that may have already been answered, but outside of the change management process. Delays now occur as the change is scrutinised for the first time and chances are that there may be conflicts with the intended change implementation date and other changes that are scheduled. The change implementer becomes "piggy-in-the-middle" between the business applying pressure for the change to go ahead as intended and the change management process delaying implementation. Change management is seen a bottleneck, bureaucratic and simply a hindrance to service improvement.

***The true value of change management will only be realised when it is a lifecycle process, all those involved in change know what is required at each stage of the lifecycle from a change management perspective and there are no surprises along the way.***

### 3.2 Project Management and the Change Schedule

In many organisations there are two distinct processes – change management and project management and often no integration between the two. "Changes" are handled via the change management process and projects managed via the project management process. Inevitably clashes and conflicts occur as both changes and projects compete for the same resources and timeslots.

Project management is simply an approach that is adopted to manage a change of a particular size, complexity or risk to the organisation. In other words a project is just a large or complex change. Projects should be initiated via the change management process just as any other change should be and the associated change record linked to the project details. In this way all changes are visible regardless of how they are being managed.

All changes, including those being managed as projects, should be on a change schedule so that resources can be allocated accordingly, test environments made available as needed, and implementation dates scheduled.

This will avoid the situation where the project team come in to work at a weekend to implement a change only to find that the network is unavailable due to some scheduled maintenance. The left hand didn't know what the right hand was doing!

The change schedule should be circulated as widely as possible so that everyone is aware of what has been planned. Even if it is only tentative dates that are known at the start of a change or project, these should be placed on the change schedule to raise awareness of the intent. The change schedule should be visible to the business, and external as well as internal service provider groups.

As well as all the changes including projects, the change schedule should include scheduled maintenance windows and any change-freeze (or blackout) periods. Work being carried out by external service providers that may impact the organisation should also be included. The change schedule calendar should extend as far as possible that is reasonable to be managed. This will vary from organisation to organisation and be influenced by the volatility and degree of change taking place in each. However, every effort should be made to lock down the change schedule as much as possible for the next 2-3 months and then dates beyond that will be tentative and subject to change.

### **3.3 Education, Awareness and Continual Improvement**

One reason for failure of the change management process I come across in many organisations is simply a lack of awareness or education. Those tasked with the delivery of changes are just not aware of what the change management process is and what is required of them.

When the process was first established there might have been some level of education and awareness carried out but this has not been maintained. New people have come into the organisation and they have not received the required education and awareness of the process. They do not understand the reason for change management, the benefits, the process and activities to be carried out and more importantly of all – what's in it for me (WIIFM).

Without establishing the WIIFM aspect of any process there will be little incentive for people to follow the process. The simplest WIIFM aspect of change management is that if the process has been followed and something goes wrong with the change, you have covered your back. If you have not followed due process and something goes wrong with the change, expect to be held responsible and to be asked hard questions.

Change management is often not "sold" in this way and individuals fail to see why they should follow the process. It is often seen as an unnecessary overhead and a hindrance to getting the job done. The process owner for change management has an obligation to make sure there is wide understanding of the process, the objectives are clear and everyone has buy-in – without exception. See section: 3.4. Zero Tolerance and Organisational Culture.

An ongoing education and awareness programme should be run across the organisation. Everyone should be encouraged to provide feedback on the process that feeds into a programme of continual improvement. All feedback should be acknowledged and responded to.

### **3.4 Zero Tolerance and Organisational Culture**

Generally people do not bypass process deliberately. They do so because they are not aware of the process, the process is a bottleneck or they are under pressure from a position of authority to bypass the process.

Every effort should be made to ensure that the process is not a bottleneck and that everyone has received the appropriate level of education and awareness.

When the process is streamlined and there is widespread understanding of change management then an organisational culture of zero-tolerance for unauthorised changes should be instigated.

I hear many organisations talk about zero-tolerance but very few 'walk-the-talk'.

I remember many years ago, listening to the Change Manager of a large financial organisation giving a presentation on the state of change management in his company. He talked about how they had introduced a policy whereby on discovery of one unauthorised change, the person responsible for the change was given a warning and on discovery of a second the person was dismissed from the organisation. This policy had been rigorously implemented and although there had been an initial downside whereby the organisation had been forced to dismiss some of their most experienced systems programmers the upside was that the instances of unauthorised changes and the number of incidents resulting from changes had reduced to near zero.

The adverse financial and reputational cost to this organisation as the result of unauthorised changes had been deemed unacceptable and appropriate action taken. Whilst I am not advocating that this line of approach would be suitable for every organisation I do believe that unauthorised changes should be investigated and hard questions asked. There should be a policy in place that everyone is aware of.

As long as the change management process that has been implemented is effective and efficient and subject to continual improvement, more organisations should be taking this approach. If there is no reason why the process should be bypassed then a tough course of action and approach is justified.

Clearly each instance of an unauthorised change should be investigated to ensure that the resulting actions are justified but where they are, policy should be adhered to. There have been numerous examples reported in the press of organisations suffering service outages and disruption to customers due to failure to follow a change management process. Organisations may be able to quantify the financial impact of these failures but the impact on brand and reputation, loss of customers and repeat business can be harder to quantify and harder to recover. Yet organisations continue to accept the situation and no-one asks the hard questions or holds anyone accountable.

In one organisation where I worked the change management process stated that when an unauthorised change was discovered and the instigator identified or a failed change occurred, an email would be sent to the owner of the change to 'please explain'. A spreadsheet was maintained with the date the email was sent and a follow-up date assigned if no response had been received. When the follow-up date was reached another email would be sent and so it continued!

There was no reduction in unauthorised or failed changes as a result of this activity. In order to rectify the situation we changed the process to ask the 'please explain' question at the Change Advisory Board (CAB) meeting and it was minuted that the person accountable would have to provide feedback at the next meeting. At the same time we also raised the authority level of the CAB by including a direct representative of the CIO. If feedback from the person accountable was not

received or an acceptable explanation received the issue was escalated up the management chain.

This simple change in process resulted in a drastic reduction in unauthorised and failed changes. People were being held accountable for their actions and as a result behaviours also started to change.

### 3.5 Management Commitment

I am always reluctant to use the term 'management commitment' as it is overused and too much emphasis is put on the need for total management commitment in order for changes to be made within an organisation. However, following on from the last section on 'Zero Tolerance and Organisational Culture' I believe that it is worthy of a mention.

There has to be management commitment or management buy-in to the change management policies and processes. Everyone regardless of rank within the organisation has to be subject to the same rules and regulations. In other words there is no bypassing of the process because you have a level of seniority in the organisation. When the process is overridden by a manager who believes he/she is above the 'law' the process loses all credibility.

This is not to say that processes should not cater for requests that come from VIP staff and that they are given a higher priority than some other requests. This is an organisational decision but as long as it is written into the process parameters then it is an integral part of an agreed process. Most often these will be a part of the request fulfilment process and not the change management process but the same rules should apply to all processes.

I could write another paper on how to get management buy-in but essentially it is about fostering a culture of cooperation and collaboration; it is about garnering an understanding of why policies and processes are necessary and the implications if they are bypassed; it is about establishing the WIIFM position so that there are perceived personal advantages in adhering to processes.

Marketing is not an area that we are necessarily good at in IT but essentially that is what is required. We need to be able to sell the reason for policies and processes right across the organisation. We need to identify the various stakeholders and mould our message to appeal to the different audiences and their vested interests.

### 3.6 The CAB

There are a number of aspects around the structure and the conduct of the Change Advisory Board (CAB) that I have observed having a detrimental impact on the change management process. Most of them are really about applying some common sense.

The CAB should only need to assess and approve or reject the minority of changes that are taking place within the organisation. We have had the concept of "standard changes" in ITIL for some time now. These are the changes that are pre-authorised due to their low risk, the fact that they are relatively common and they follow a predefined procedure or work instruction. More and more changes should fall into this category and not be a concern of the CAB. See section: 3.11 Streamline.

The technical assessment, risk assessment, business impact assessment etc. for other changes should be done outside of the CAB and the results reported to the CAB. CABs that attempt to do this within the forum end up running for hours if not days and attendance will rapidly diminish.

Some organisations have sub-committees or technical review boards that perform the technical assessment of changes before they are submitted to the CAB. Service Owners or Business Relationship Managers should be performing business impact assessments with the business and reporting on findings to the CAB.

All changes that require CAB assessment should be circulated to the membership before hand and the meeting should be managed by exception. The only changes that need to be discussed are those that have raised any concerns or questions.

Where there are scheduling conflicts that arise between changes, the Change Manager should make an arbitrary decision based on the priority of the changes and report that decision to the CAB for ratification. The CAB may decide to overturn the decision but once again it is management by exception.

The CAB does not have to be comprised of the same people for every meeting. There will be a core of regular attendees including the Change Manager but the only people at the CAB should be those that have a vested interest in the changes that have been tabled. If people are asked to attend a meeting in which they have no vested interest they will stop attending or delegate downwards which brings me on to my next point. The CAB needs to be flexible!

The CAB should have enough seniority or authority to make decisions and hold people accountable. The CAB is operating on behalf of the CIO to ensure that changes are controlled and made with minimum disruption to IT services. Therefore the attendees should be able to make decisions on behalf of the CIO. If the requested attendees start to delegate their attendance on a regular basis it is most likely that the meetings are taking too long or that they are being asked to attend meetings to which they have no input.

It is amazing that despite the advancement in technology so many IT organisations still insist on holding their CAB meetings physically! Many years ago I came across an organisation that were quite successful in carrying out their CAB meetings via email but they were the exception to the rule. CAB meetings can be virtual meetings using collaboration tools and social media channels. They become far more effective and efficient and people will participate. It is time for IT to take advantage of the technology that it provides!

### **3.7 The ECAB**

The emergency CAB or ECAB is also a concept that I have seen over engineered so it just becomes a bottleneck and a hindrance to getting things done. Emergency changes should be the exception to the rule. The number of emergency changes should be monitored and measured and action taken to reduce the frequency. See section: 3.9 Monitor, Measure and Act.

If we are not causing things to fail as the result of changes i.e. we get things right first time through proper design, build and test, then ideally emergency changes should only be required when there are failures in infrastructure and immediate repairs needed to restore service. However in the real world in which we live there will be other reasons for emergency changes. Human error will occur and result in the need for immediate intervention.

The ECAB just like the CAB does not have to be physically meeting of people to make a decision on whether the change should be approved or not. It may be just a telephone conversation between one or two people who have been given delegated authority to act as the approval body for emergency changes.

Not all emergency changes may need ECAB involvement. Many emergency changes may be those that can be expected and the resolution for which is well understood e.g. server hardware replacement. ECAB authority for approval of these changes can be delegated to operational staff who are available at the time that authorisation is required.

In fact the most effective way in which to operate an ECAB is to delegate authority to a number of individuals who have the seniority to make a decision. The role of these individuals in the event of an emergency change being needed is not necessarily to make a detailed technical assessment of the change being proposed. The person proposing the change will hopefully have done this and be able to articulate the outcome of the assessment. The role of the person representing the ECAB is to ensure that all considerations have been taken and ask the questions that are often overlooked in emergency situations when service is down or service outage is likely to result if immediate action is not taken. These questions include:

- What is the impact if this emergency change does not take place? Is it really an emergency?
- What services are currently impacted?
- What service will be impacted and when?
- How long will the change take?
- What additional resources / assistance are needed?
- Is there a back-out plan if the change does not work?

Once it has been established that all due considerations have been made and that the need for change and associated risk is acceptable, the change can be implemented whilst appropriate notifications and escalations are put in place. Make sure that the collective of individuals who have ECAB authority can provide coverage across the time periods for which they may be required i.e. there is always an ECAB representative available to be contacted.

### **3.8 Risk Assessment**

Despite plenty of guidance on ways in which to conduct risk assessments both in ITIL and elsewhere including Management of Risk (M\_o\_R), ISO 31000, ISO 27001 and from bodies such as ISACA, many organisations do not subject changes to a risk assessment unless they are managed by a project management methodology which requires a risk assessment to have taken place.

No change is without risk and therefore all changes should be subject to a risk assessment as a part of the change evaluation to determine potential impact on the business, service level targets, corporate objectives and policies, other changes etc. The level of risk assigned to a change will determine the level of due care and attention that the change requires. All changes should be assessed for risk from a business perspective, which can have a very different outcome than a risk assessment focussed on the technology perspective.

For many changes all that is needed is a simple change impact and risk assessment matrix. ITIL has an example and there are many available on the internet.

It does not need to be a complex process but unless each change is subject to a risk assessment the change cannot be properly evaluated and adverse impact avoided.

### 3.9 Monitor, Measure and Act

If the change management process is to be a success it should, as any other process, be subject to continual improvement. This means that the process should be closely monitored and measured, and action taken to instigate improvements.

Changes that are submitted for evaluation and are rejected should be analysed. The reasons for rejection should be reviewed and action taken where the reasons for rejection can be mitigated. I have worked in organisations where changes continually get rejected because all of the required fields on the Request for Change (RFC) have not been completed. The change requestor gets more and more frustrated and this can result in the process being bypassed because of pressure to get the change processed. In most situations this can be rectified with education and awareness so that all change initiators are aware of the requirements of the process and the reason for those requirements. However, it could also be a matter of improving the RFC form!

Continual feedback from those involved in the change management process should be sought and opportunities to improve the process taken. Where bottlenecks, excessive administration or high levels of perceived bureaucracy are identified, action should be taken to remove them.

The number of emergency changes should be monitored and measured and action taken to reduce the number over time. Emergency changes by their nature are the ones most likely to be disruptive and prone to failure and therefore every effort should be made to avoid them. Checks should be made to ensure that changes being lodged as emergency changes are genuinely emergencies and not the result of poor planning.

Incidents that are the result of changes should be reviewed and analysed to determine why the change had an unintended adverse impact. Efforts should be made to reduce the number of incidents resulting from change over time.

Opportunities to improve the change management process should be discussed at the CAB. Feedback on the process should be sought from across the organisation including the business as well as IT. Actions to improve the process should be documented and progress tracked and reviewed by the CAB.

Post implementation reviews of changes should capture 'lessons learnt' so that these can be fed into future changes. The review should confirm that the change has met its intended objectives, that all stakeholders are satisfied with the outcome and that there have been no unexpected side-effects from the change. Even if this cannot be done for all changes, the change management process should ensure that this is done for a sample of changes on a regular basis e.g. spot-checks are performed.

### 3.10 Accountability

The change management process is often set up to fail, as the expectations are that the process and process owner will be held accountable for changes that fail or have an adverse impact on service delivery.

The change management process is responsible for ensuring that changes are evaluated and if authorised, subsequently designed, built, tested, implemented and reviewed.

The ultimate responsibility, or accountability, for the quality of the change rests with the Service Owner of the service being changed. The Service Owner should have been involved with the change throughout its lifecycle and should be represented at the CAB and any other change authority.

When the Service Owners are subject to this accountability, greater scrutiny and due care and attention will be given to changes being made.

### 3.11 Streamline

The concept of a standard change has already been discussed in section 3.6 The CAB. A standard change is a change to a service or other configuration item for which the approach is pre-authorised by change management, and this approach follows an accepted or established procedure to provide a specific change requirement.

Every standard change should have a change model that defines the steps to follow, including how the change should be logged and managed as well as how it should be implemented.

Many organisations identify some standard changes when establishing the change management process for the first time. The objective is to promote efficiency and avoid the change management process having high levels of administration and therefore resistance to the process.

However, few organisations make the identification of standard changes a regular occurrence. There should be a process by which recurring changes are assessed to determine whether they can become standard changes. As much use as possible of devolved authorisation through the standard change procedure should be a key objective.

Each change should be assessed to determine whether there is a defined trigger that initiates the change e.g. a service request or exception from event management; the tasks to implement the change are understood, clearly documented and have been proven; all stakeholders are in agreement that authority for the change can be given in advance; the cost of the change is known and accepted or authorisation to incur the cost placed in the control of the change requester; and the risk is low and well understood.

Where these criteria are met, or can be met, the change should become a standard change and therefore the change management process continues to be streamlined. Overheads are reduced and the process becomes more effective and efficient.

It is only in this way whereby the CAB has less and less to do in regards to change assessment will there be widespread acceptance and adherence to the process. When the CAB membership is called on repeatedly to assess and authorise the same types of changes on a regular basis there will be dissatisfaction and the chances are that participation will dwindle.

### 3.12 Service Asset and Configuration Management

No discussion on the failure of change management would be complete without mention of Service Asset and Configuration Management (SACM). Many changes fail and result in incidents due to the inability to perform proper impact assessment. Without the existence of a Configuration Management System (CMS) that is accurate and comprehensive, most impact assessments are reliant on the knowledge held by individuals. This is flawed and subject to human error.

Change management like many of the other service management processes will only reach a level of required maturity with the support of a CMS.

Organisations that are serious about raising the quality of their service provision through improved service management processes will invest in the implementation and maintenance of a CMS.

### 3.13 Service Provider Groups

The change management process needs to incorporate both internal and external service provider groups.

Most organisations have a number of external vendors and suppliers who are providing services. The change management process must ensure that it encompasses these third parties to ensure delivery of service to the business as expected.

The failure to include third parties in the change management process can lead to changes taking place without due consideration and proper evaluation. Change conflicts can occur, and at worst service outages.

Change management should also work with supplier management to assess the change management processes within supplier organisations to be assured that the suppliers themselves have processes in place to manage changes effectively.

### 3.14 Technology Exploitation

It is my experience that many organisations simply do not take advantage of the technology that they have available to them. I have already mentioned in this paper the collaboration tools and social media channels that can be used to make the assessment of changes more effective and efficient.

It is also often the case that the full capabilities of the service management tools and technology purchased by an organisation are not being used. Many tools will assist with prioritisation of changes, risk assessment, standard change models, scheduling and conflict resolution, linkage of changes to projects and vice versa which are all aspects of change management that I have discussed as sometimes problematic.

I recommend that organisations not only look at how they can improve the service management processes including change management but also how the technology they have available to them can be leveraged to help. Talk to the vendor of your service management tool and ask them what their offering can do to help.

#### 4 CONCLUSION

The IT service management industry has 'favours of the month' when it comes to processes. A few years ago it was configuration management and before that it was service level management. Now it is service catalogue management.

I think we should take a step back and go back to basics. We should take another look at some of the less 'sexy' processes that have been around for a long time and make sure that they are working effectively and efficiently before deciding to move on to the next process initiative.

The reality is that if your basic processes like incident and change management are not working effectively, the rest of your processes are likely to be failing too. All processes should be subject to incident and change management just as infrastructure and applications are. Therefore if these basic processes are not working, how can we manage issues or improvements to the other processes?

So, I encourage organisations to take a look at where they would fall if they were to answer the question posed by the Forrester survey – 'what percent of your incidents are the result of change?' If you can answer 'less than 10%' then well done. If you are anywhere else then you need to determine why your change management process is failing you. Hopefully some of the suggestions in this paper will be able to assist.

Karen Ferris is a Director at Macanta Consulting. She has been in the IT Service Management industry since 1994 and has worked as a practitioner, manager, trainer and consultant. She is a board member of itSMF Australia, Fellow of priSM and a member of the international Editorial Advisory Taskforce working on the itSMF library. In 2007 she was bestowed with the inaugural Service Management Champion award by itSMF Australia. Karen is a sought after international keynote speaker and is the author of the 2011 publication 'Balanced Diversity – A Portfolio Approach to Organisational Change'. She was a contributing author to the "Greening Service Management" book.

Karen can be contacted at [Karen.ferris@macanta.com.au](mailto:Karen.ferris@macanta.com.au).