Article Paper

Preventing ‘value leakage’ through the effective and efficient handling of major incidents

Submitted by:
Mark Sykes
Principal Consultant
and
Avinash Singh
Country Manager, Fox IT India

Office: +44 (0) 333 202 1018
Email: mark.sykes@foxitsm.com

Email: avinash.singh@foxitsm.com

Introduction

With the ever increasing reliance on information technology for delivering services, the associated costs when things go wrong can have a significant impact on the business and of the organisation as a whole. A major incident could result in a loss of revenue, cause regulatory non-compliance/non-conformance (potentially resulting in financial penalties), generate reputational damage, impact staff productivity, incur additional support costs in remediating the issue, etc.

Aspects such as these, also known as **value leakage**, can together carry a heavy financial burden and hence minimising the occurrence of major incidents, or reducing their duration when they do occur, should be seen as an improvement imperative that can generate substantial business benefit for organisations aspiring to reduce or minimise their value leakage through the effective and efficient handling of major incidents.

This paper outlines some of the mechanisms that should be utilised to help deliver an improvement in how major incidents are handled. A variety of concepts, tools, methodologies, techniques, etc. are also mentioned, including ITIL®[1], ISO/IEC 20000, Agile, as well as Fox IT®[2] specific services like FoxPRISM™ and FoxMAPS™. Using a combination of these to implement something that best fits your organisation will help to begin to address any value leakage being experienced.

Criteria for identifying a major incident

Before we take a look at the handling of major incidents, first we have to focus on identifying when a major incident has occurred. Rather than relying on customers and users contacting a Service Desk to report a fault with a service, early identification is a key factor in helping to minimise disruptions. Technology opportunities need to be maximised, with the use of systems management, event monitoring, and artificial intelligence tools amongst those that can enhance the detection capability of a major incident.

Having clearly defined criteria written in language that stakeholders can understand is vitally important in being able to determine when a Major Incident Management process should be triggered. When drafting the criteria, review previous major incidents and serious issues that have occurred. Being able to relate criteria to real-life scenarios will help support teams such as the Service Desk make a more speedy and accurate judgement that a major incident has occurred. ITIL® 4 propagates the notion of the 'shift-left technique' and hence providing teams like the Service Desk with the tools and knowledge to rapidly identify when a major incident arises will help to keep the end-to-end duration of a major incident to a minimum.

Other criteria that may need to be considered is the time of day, week, month or year that an incident occurs. The end of the month, key public holidays, or other critical business periods can often be an important time when an incident may take on greater significance because the business impact may be more severe. More obviously, a typical service-impacting incident that occurs outside normal business hours may not need to be handled the same as if it occurred during business hours.

Serious issues may initially be identified via avenues such as a customer contacting a Service Desk or automated monitoring tools detecting a critical event. Each of these will need reviewing and validating to confirm the issue is indeed first and foremost an incident, and that it meets the criteria for being a **major** incident.

The incident should be recorded in an IT service management (ITSM) toolset just like any other incident that occurs. Its impact and urgency will need to be assessed, from which the priority of the incident can be allocated. In the experience of Fox IT, organisations typically prioritise incidents based on a rating system that ranges between a priority of P1 through to P4, with P1 being reserved for incidents of the highest level of impact and urgency. That being said, not all P1 incidents are necessarily major incidents. This is where additional criteria need to be available to objectively determine the subset of P1 incidents that will be categorised as major incidents.

[1] ITIL® is a registered trademark of AXELOS Limited
[2] Fox IT® is a registered trademark of Fox IT SM Limited

Major incident management policy

Having a policy for Major Incident Management can be a useful artefact for including a reference to the criteria for determining when an incident is to be categorised as a major incident. A policy document should also contain mandatory statements in respect of how major incidents will be handled, the interfaces and triggers to other processes, timeliness for carrying out major incident reviews, etc.

Identifying incident records as 'major incidents'

An ITSM toolset should be configured such that major incidents can be readily identified amongst all the other incidents that are recorded. This can simply be a checkbox on an incident record that someone can tick once the identification of a major incident has been confirmed. The checkbox should be easily visible within the record and able to be reported on (for example, if wanting to show a report of all major incidents that have occurred in the last period).

'Parent/Child' incident records

Often times when a major incident occurs, many calls are received to a Service Desk and multiple incident records are created that are all related to the single issue that has arisen. In this scenario, it is best to select one incident record (typically the first one that was recorded in the ITSM toolset) and to identify it as the 'master' or 'parent' record. All other incident records related to the major incident should then be linked to this record; this builds a parent/child relationship between the records. Then, only the parent record needs to be kept up-to-date with the specific investigative and resolution activities that take place.

When configuring an ITSM toolset, this latter capability is extremely useful when handling a major incident that result in lots of related incident records being created. Rather than having to update multiple records, the parent record can be just the single record that is manually kept up-to-date.

Ideally, the toolset should be configured such that when the parent record is resolved, all of the related child records are automatically moved into a resolved state (and relevant data fields such as the resolution information copied over into each individual child record). This can save a lot of human effort, whilst at the same time preserving the integrity of data in respect of the number of incidents that have been reported in relation to a major incident.

Human resources for handling a major incident

Once the occurrence of a major incident has been confirmed, it is important that appropriate human resources are assigned for managing, investigating and resolving it. The intention here is to ensure that these stakeholders can be solely focused on the major incident and not have any distractions from their normal daily activities. One way this can be achieved is to hand over the management of a major incident to an individual who will perform the role of Major Incident Manager.

Major Incident Manager

Each major incident should be assigned to someone that will have the responsibility for managing it through to its conclusion. This role, known as the Major Incident Manager, provides a single focal point for ensuring that all necessary parties are involved in the investigation and resolution of the major incident, as well as making sure that correct and timely communications occur to all relevant stakeholders.

Depending on circumstances, such as the day and time that the major incident occurs, the role of Major Incident Manager may be fulfilled by an individual performing another role, such as the Service Desk Manager, Operations Manager, Problem Manager, etc. Some organisations may have employees that provide a dedicated role of Major Incident Manager.

Irrespective of the individual fulfilling the role of Major Incident Manager, the applicable policy, process and procedures will be the same.

For organisations certified, or seeking certification, to ISO/IEC 20000, having an individual assigned the responsibility for managing each major incident is mandatory. This does not have to be a single person with a specific responsibility for managing all major incidents, but each time a major incident arises, someone needs to be assigned for its management.

Major Incident Response Team

Depending upon the type of major incident and its impact (such as the affected services, infrastructure and customers), it can often be beneficial to construct a cross-functional team that is comprised of members with relevant expertise and knowledge based on the specific circumstances that have arisen. Nominally known as a Major Incident Response Team (MIRT), this is a good mechanism for ensuring that the correct resources are focused on the active major incident and that team members are not distracted by other less pressing matters. Here, a methodology discussed in ITIL® 4 and known as 'intelligent swarming' can be utilised not only as a mechanism for gathering together the right personnel with the right skills and competencies, but also for promoting collaboration within the team rather than competition against one another.

The Major Incident Manager (MIM) has a responsibility for determining the core members of this team and coordinates these resources and the activities that they are undertaking (both during the investigation and resolution of the major incident). Providing oversight and coordination of the activities that are taking place gives the MIM visibility of when additional resources need to be brought into the MIRT as circumstances dictate (including drafting in the assistance of third parties, as required). The MIM taking care of this responsibility is another example where MIRT members can concentrate their focus on performing their respective activities.

Critical Situation Room

In keeping with the principle of the MIRT being able to focus on the major incident and not be distracted by unrelated things, it is often beneficial to have the team located together in a workspace where needless interruptions can be minimised. It is therefore recommended that a predefined or allocated space be made available where the team can all come together and work on the major incident as a whole, single team.

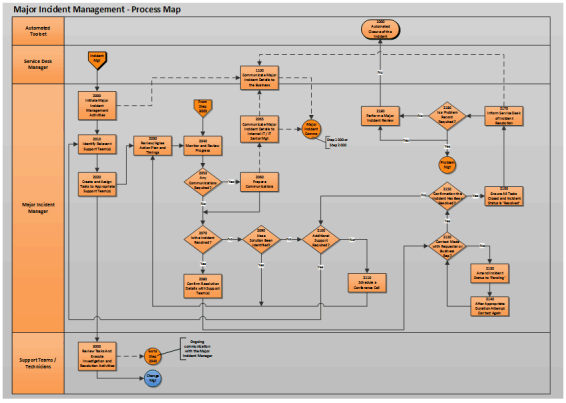
Having a space such as this where all team members can come together as one can help to improve communications across the various functional teams involved, and it will certainly help the Major Incident Manager maintain a good level of oversight and awareness of the respective team activities that are being undertaken.

In an ideal scenario, this workspace should be located near to the epicentre where any related incidents are incoming, such as the Service Desk or Network Operations Centre. This will make communications back and forth that much easier and quicker, and particularly where there is a direct customer impact, rapid feedback will be vital to the MIRT as the team handles the major incident (e.g. monitoring ongoing impact, assessing the success of potential resolutions, etc.).

Maintaining an Audit Trail

All parties involved in handling the major incident, whether its investigation or resolution, needs to ensure that an accurate audit trail is maintained throughout their respective activities. Everyone needs to ensure that the 'parent' major incident record is kept up-to-date with the activities that have been undertaken and the date/time that they were performed. This data will be vital input when a review of the incident is undertaken subsequent to its resolution or when a root cause analysis is done (usually as part of the Problem Management process).

Process and procedures



Another key factor for any organisation in helping to minimise value leakage is to have a defined process (and accompanying procedures) in place for the management of major incidents, and to ensure that relevant stakeholders are familiar with their role within the process. This recognition by all parties can help to ensure there is no misinterpretation or miscommunication of roles and responsibilities – issues that can often arise when dealing with the pressure of handling an active major incident.

FoxPRISM™, Fox IT's fully interactive and customisable web-based process knowledge database (and which assists in the design, implementation and management of service management processes), features a Major Incident Management process that can be used by an organisation as a framework for providing tighter control and better oversight of the many activities that are likely to be undertaken during the lifecycle of a major incident.

Important interfaces for any Major Incident Management process are those to Change Management and Problem Management. Change Management so that any change requests are raised and approved prior to implementing a fix to resolve the major incident, and Problem Management to ensure that an analysis of the major incident is performed, and its root cause attempted to be identified.

Procedures

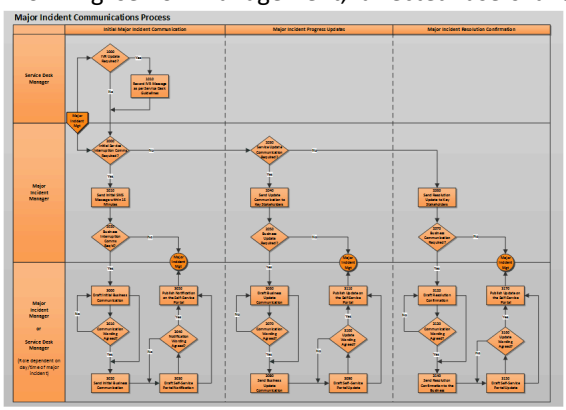
Along with the process, having a set of associated procedures is another important aspect that can help facilitate more effective and efficient handling of major incidents. Procedures need to include relevant escalation activities, including:

- **Functional escalation** for engaging with technical support teams when expert guidance is required for the investigation and resolution of a major incident (including both internal and external parties).
- **Hierarchical escalation** for informing senior management on the occurrence of a major incident, or if needing to seek additional resources when service level targets are in danger of being breached (or indeed have breached).

With 'intelligent swarming' mentioned earlier in the description of the Major Incident Response Team, procedures should also exist where this methodology can be promptly initiated, providing the organisation with a re-assurance that the most suitable MIRT members will be swiftly engaged with.

Communication

Communication is a vital element when managing a major incident and is another key responsibility for the role of Major Incident Manager (MIM). Informing senior management, affected users and customers, and other relevant stakeholders when a major incident occurs and then keeping them informed of progress (including the ultimate resolution and restoration of service) is such an important facet of Major Incident Management, that it is often worth defining a separate communications process to cover all of the necessary activities.



FoxPRISM™ features a Major Incident Communications (MIC) process that an organisation can utilise to better structure and manage the communications that need to be delivered to a wide variety of stakeholders during the lifecycle of a major incident.

Along with the associated procedures, having a MIC process can help to ensure that everyone is informed not only when a major incident arises, but also that they are regularly updated during the progress of the major incident, and on its resolution and the restoration of service.

Often times, managing a major incident can lead to increased stress levels. Panic can set in if the major incident drags on longer than anticipated; senior management can exert undue additional pressure; affected customers can be vocal in their complaints; etc. Having a process and procedures that are clearly defined can help to ensure communications are delivered in a concise yet proactive manner and enables the MIM to exude a confidence that the situation is under control and being managed appropriately.

Communication tools

An important facet of communicating in an effective and efficient manner is having the right tools in place. Make sure best use is made of the latest technologies, whether that be SMS text messages, push notifications within an app, social media channels like Twitter, etc. Integrating (where possible) aspects like these within an ITSM toolset will also help facilitate better tracking and management of communications.

Performing a major incident review

After the resolution of a major incident it is important that a review is undertaken that looks at a number of factors, including:

- What exactly happened (including symptoms, how it manifested itself, etc.)
- The service impact along with who the affected customers/users/other stakeholders were
- How quickly it was detected (e.g. do systems management/monitoring tools need enhancing)
- What activities were undertaken to resolve the major incident and restore service
- Why did it happen (i.e. the root cause – if known at that stage)
- What actions are needed to prevent a re-occurrence
- Other improvement recommendations (in areas such as people, process, technology)
- Outage start and end time; total outage duration
- Financial cost of the major incident

Sometimes called a 'post mortem', it is important that the nature of the major incident is fully understood and that improvement opportunities are identified. Improvements could potentially be in a number of areas, for example: changes to how functional escalations are handled; enhancing the levels of redundancy in infrastructure components; implementing technical solutions for the earlier identification of major incidents; etc.

The review may be performed by the Major Incident Manager, but if a completely objective view is required then it can often be more appropriate for the Problem Manager to facilitate it. Ensure that all relevant stakeholders are engaged in the review so that there is comprehensive input across all areas that have been involved in handling and managing the major incident.

Following completion of the review, a major incident report (containing the factors listed above) should be published to relevant stakeholders. Subsequent actions need to be clearly assigned and then tracked through to conclusion. This latter action of tracking the improvements is often best served by being the responsibility of the Problem Manager.

It is recommended that each major incident record is associated to a problem record to ensure that the root cause is suitably investigated. This could be a new problem record but equally it could be an existing problem record should one already exist for the type of major incident that has occurred.

Retrospectives

Organisations that practice agile or scrum methodologies will be familiar with carrying out so-called retrospectives to identify new learning opportunities. Major incident reviews are similar exercises in principle, and hence existing practices and procedures can be re-utilised rather than creating a new review mechanism from scratch.

Practicing readiness for a major incident

It is important that an organisation is fully prepared for when a major incident occurs. It's safe to say that for the majority of organisations it isn't a case of **if** a major incident will occur, but actually **when** one will occur. On that basis, having tried and tested processes and procedures in place will increase the readiness of the organisation to handle major incidents in the most efficient and effective manner possible.

On a regular basis, simulations or mock drills should be undertaken for different types of major incident that an organisation could suffer from. These could be real-life examples of ones that have occurred previously, or hypothetical ones that could likely occur. For some fortunate organisations, major incidents may be a very rare occurrence, and more imagination may have to be used. In this scenario, it may be a useful idea to take a selection of incidents prioritised as P1 or P2 and handle them as if they were a major incident. This can be useful in validating both process and procedures and can also introduce a level of realism into the exercises rather than just relying on purely hypothetical examples.

It may also be prudent to review the output of risk assessments and business impact analyses as this may provide items for consideration when performing the simulation exercises. Equally, don't feel it is absolutely necessary to accurately reflect the technical elements of a failure that causes a major incident; often benefits can be realised just by performing classroom-based 'table-top' exercises.

The regularity for carrying out these exercises will vary for each organisation. Ideally, they should take place at least annually, but the frequency may to some extent be determined by how regular real-life major incidents occur. Any associated major incident restoration/recovery plans should also be kept under regular review (and re-tested when appropriate), particularly as new services are introduced or major changes to the infrastructure are implemented.

Calculating the cost of a major incident

Every major incident will have a cost. Even a major incident that occurs outside of normal service hours and hence has no customer impact, will still cost an organisation money in its resolution. Identifying the true cost of a major incident, or at least making a best guess estimate, can help to focus minds and efforts in seeking improvements to minimise the occurrence of major incidents or to reduce the time it takes to recover from a major incident.

In order to calculate the cost of a major incident, three key factors need to be determined:

- Loss of revenue based on the total number of minutes the service was unavailable
- Cost of reduced or loss of productivity for staff during service unavailability
- Any compensation likely to be paid to affected customers

Loss of revenue versus loss of productivity

It should be noted that loss of revenue versus loss of productivity will likely swing in one direction more than the other depending on the type of the service, i.e. whether it is a revenue generating service or one that's intended for internal consumption (by the organisation) only. For example, some major incidents may result in no loss of revenue but will have a high cost in respect of the loss of staff productivity. A good example here perhaps is a production line for new cars – if this halts for 1 hour then I suspect there is no direct loss of revenue (because maybe they can extend working hours at the end of the day to catch up), but the productivity loss would be significant.

Occasionally both revenue and productivity will be impacted – a good example of this are the recent issues with the Boeing 737-MAX 8 and MAX 9 aeroplanes following two crashes caused by suspected software-related issues. At least one airline withdrew its order for new aircraft (loss of revenue) and Boeing staff were having to focus on investigating the two crashes and fixing the faults (loss of productivity). Plus, on top of this, is the compensation that Boeing will have to pay out.

The cost of compensation

Many banks in recent years have had to pay out billions in compensation due to various mis-selling activities as well as when IT issues arise. As with the Boeing example above, this can be a significant cost to the organisation, and should not be underestimated when calculating the overall cost of a major

incident. Even if, at the time of producing a major incident report, it is only a best guess estimate, it should still be factored into the overall cost calculations.

Never underestimate the true cost of value leakage

Of course, it may take a while for a full picture to emerge of the cost of a major incident, and hence the true cost of value leakage. There are many variables to be factored in, such as the revenue, productivity and compensation impact already mentioned, but on top of this there may financial penalties, a drop in share price, customers going elsewhere, etc.

To bring some perspective to this, consider these recent examples of major incidents that have occurred:

- In 2018 TSB bank in the UK encountered a massive IT failure as a result of a failed upgrade. When the company reported their financial results, they stated that £330m was spent in addressing the IT failure, comprising of £125m in customer pay-outs, £49m in fraud and operational losses, £122m for fixing the actual IT fault, and £34m in income lost due to waived fees and charges incurred because of the disruption. It also resulted in 80,000 customers switching their account to a competitor.
- In 2017 British Airways experienced a serious IT failure, with the chief executive reporting that the company was expected to incur costs of £80m. The failure itself resulted in 726 flights being cancelled over three days with some 75,000 passengers affected.

Summary

For most organisations major incidents are a fact of life. Usually, the occurrence of major incidents cannot be 100% eliminated, therefore minimising the number of times that they do occur and reducing the time it takes to resolve a major incident and restore service back to normal operation are key aspects in lessening the cost impact to the organisation.

Whilst having the right (for example) infrastructure in place, such as increased redundancy to deal with component failures, can help to minimise the occurrence of major incidents, not being able to completely eradicate them means that an organisation needs to be fully prepared for when they do arise. In that way, an organisation can maximise the efficiency and effectiveness of how major incidents are handled – and hopefully minimise their duration.

All organisations should have policies, processes and procedures in place for handling major incidents. There needs to be a constant state of readiness – all parties involved in handling a major incident need to be cognisant of their role and their responsibilities when called upon. By definition, major incidents occur when critical situations arise, but having stakeholders rehearsed and ready to carry out their duties as expected can help to decrease the pressure and stress levels of those involved in the resolution and recovery of a major incident.

Whilst recognising that the occurrence of major incidents can never be totally eliminated, hopefully implementing some of the ideas contained within this paper will help lead to an improved management of them when they do arise; and perhaps a proportion of them can be eliminated (via the identification and remediation of root causes).

One of the ways that Fox IT can assist an organisation is via our FoxMAPS™ service. Focused just on Major Incident Management, an assessment exercise takes place that reviews the current activities for handling major incidents and determines the current level of process maturity. With output that includes a detailed report highlighting observations, strengths and weaknesses, this can be used to devise and implement an improvement programme that will begin to reduce an organisation's value leakage.

The FoxMAPS™ service can also be undertaken for many other ITSM processes, further details of which can be found below.

Mark Sykes

Principal Consultant at Fox IT

About Mark Sykes

Mark Sykes has been with Fox IT for 18 years and offers excellent all-round experience as a service management professional having been in the ITSM industry for over 30 years. Particularly strong in the Service Transition and Service Operation aspects of ITIL®, he has become one of the company's most experienced practising consultants. This includes having performed lengthy engagements as Lead Consultant in the UK, USA and Middle East as well as experience of working in other foreign territories including Europe, North and South Africa, and Asia.

Mark is Fox IT's leading process designer, helping many clients develop, re-engineer and implement processes to improve their service delivery, and then to subsequently ensure that there is ITSM toolset alignment. Additionally, Mark has supported numerous clients attain ISO/IEC 20000 certification, and currently sits on the BSI committee contributing to the revisions of this international standard. Mark also has experience of MOF, COBIT®, ISO/IEC 27001 and Sarbanes-Oxley.

Mark currently holds the ITIL® Expert, ISO/IEC 20000 Consultant, COBIT® 5 Foundation and COBIT® 5 Implementation Certificates, and has authored numerous white papers and articles. He has twice been a finalist for the 'Submission of the Year' award that is presented at the annual itSMF Service Management Industry Awards show.

About FoxPRISM™

FoxPRISM™ is a fully interactive process tool that helps our clients with the design, implementation and management of service management processes. It delivers a detailed knowledge base for users to acquire and follow key policy and processes (to level 4 procedures) to drive efficiency and productivity to the business.

Supporting process improvement and implementation

FoxPRISM™ provides a customisable framework onto which an organisation can map and build their own process models. The process and sub-process maps are designed to be easily customisable so that they become organisation-specific and subsequently provide an accurate representation of the current and/or future state way of working.

In addition to the process models, FoxPRISM™ also has a repository of over 150 supporting documents and templates, such as policies, plans, service level agreements, operational level agreements, service catalogue, risk register, job descriptions, metrics and key performance indicators, etc.

Whether used before, during or after an implementation of service management processes and/or supporting technology, FoxPRISM™ will help deliver lower cost and earlier business benefits, via:

- Accelerated implementation and improvement timeframes
- Reduced costs through more effective use of resources
- Reduced risk in using an approach based on real-life templates and many years of proven implementation experience
- More effective deployment of supporting technology via alignment to business processes
- A baseline for continuous reference and service improvement
- Knowledge repository to aid consistent use and the induction of new staff

Easy to use and understand

FoxPRISM™ is a web-based tool that is easy to customise and maintain via online access to the central platform, plus the use of MS Excel and MS Visio. Flowcharts (designed in a swimlane format) and supporting text (i.e. procedures) are combined to illustrate processes and provide a reference that can be easily accessed, maintained and understood.

It enables information to be easily shared across the entire organisation and can be utilised as a single point of reference, or indeed used as a single repository for all information.

Further information on FoxPRISM™ can be found via the following hyperlink:

https://foxitsm.com/fox-portfolio/foxprism/

About FoxMAPS™

Fox IT has developed an innovative range of maturity and compliance assessment services, commonly known as FoxMAPS™ to provide you with an independent and objective view of your organisation's maturity and effectiveness, leading to a roadmap for improvement. These assessments (including ITIL® / ITSM Assessments and ISO/IEC 20000 Assessments) use a structured approach to gather and analyse relevant information and then to produce the output in a format that meets your business needs.

Each FoxMAPS™ assessment also draws upon Fox IT's many years of proven implementation and improvement experience, combined with industry best practice guidelines and frameworks, such as: ITIL®, ISO/IEC 20000, MOF, COBIT®, CMM, etc.

Comprising of a combination of on-site interviews and workshops, observation of process activities in operation as well as documentation review, a FoxMAPS™ assessment not only provides a baseline from which to measure future progress, but clearly identifies the issues that need to be addressed and provides individual recommendations for their remediation.

About Fox IT®

Fox IT has been a leading information technology service management and governance business for over 30 years. We provide a range of practical and effective consultancy solutions designed to create agile, proactive, responsive IT organisations providing excellent IT services in alignment with our clients' goals to support and drive continuous business innovation. We achieve this by empowering your people with best practice training, developing and implementing the right operational processes and using properly configured and integrated tools to enable IT service transformation.

To discuss how we can assist you in transforming your IT services or in obtaining ISO/IEC 20000 certification please call us now on +44 (0) 333 202 1018.

Please come and join in the latest ITSM conversations on our social media pages:

LinkedIn Company Page: www.linkedin.com/company/fox-it

Facebook: www.facebook.com/FoxIT.ITSM

Twitter: https://twitter.com/FoxIT_ITSM