

Banks and Avian Flu: Planning for a Possible Pandemic

Abstract

An Avian Flu Pandemic would fall under one of the four categories of ‘operational risk’ defined by new Basel II banking regulations, specifically an ‘external event’. As such, banks and other regulated financial institutions are required to maintain regulatory capital to cover the financial losses that might arise from such an event, and are also required to maintain and test Business Continuity plans that would aim to mitigate the impact of such an event.

Business Continuity Planning (BCP) has become an established and respected discipline in all financial institutions, increasingly integrated with other Operational Risk Management functions. However, many of the assumptions underlying BCP planning today, based as they are around catastrophic scenarios such as 9/11, where premises and systems are suddenly knocked out of action, **will not hold in a pandemic!**

In a pandemic, it will be people rather than infrastructure that will become unavailable. And it is the largest firms, with multiple overseas offices and highly centralised support functions, which will be most at risk.

This paper is one of the first to study the potential impact of an avian flu pandemic on the operations of global banking industry and is designed to encourage critical thinking on this serious topic. As a starting point, the paper proposes practical steps for beginning to understand the operational risks resulting from a pandemic and to develop Business Continuity Plans to mitigate the detrimental impact of such a catastrophe.

Keywords

Avian Flu Pandemic,
Basel II,
Operational Risk Management,
Business Continuity Planning, BCP

The Potential for an Avian Flu Pandemic

The World Health Organization (WHO) reports that, since 2004, a growing number of Asian countries have experienced outbreaks of “avian influenza” in domestic poultry and in migratory wild birds [1]. Most of these “historically unprecedented” outbreaks have been caused by a highly pathogenic strain of influenza known as **H5N1**, which has already crossed the species barrier to infect humans, with a high rate of mortality. WHO are concerned that such outbreaks could give rise to a new influenza “**pandemic**” in humans. A pandemic could occur when avian and human influenza viruses exchange genes giving rise to a completely new subtype of the influenza virus to which few, if any, humans would have natural immunity. Unfortunately, existing influenza vaccines would not be effective against a completely new influenza virus and experts believe that it would take several months to develop an effective vaccine and the to vaccinate the population at risk.

The consequences of a pandemic are potentially very grim. The May 2005 special edition of the scientific journal Nature on Avian Flu [2] warned “tens of millions worldwide might die, leaving the global economy in tatters. The first act, the spread of avian flu to, and probably between, humans, has already started across Asia. [And] unless the international community now moves decisively to mitigate this pandemic threat, we will in all probability pay heavily within a few years.” WHO, the international body charged with tackling such outbreaks, recently recommended that “all countries, both those affected and unaffected by avian H5N1, ... should move ahead as quickly as possible and develop or finalise practical operational pandemic preparedness plans”.

The human costs of an avian flu pandemic will be devastating, with experts estimating millions of deaths worldwide, dwarfing the financial losses that will be experienced by the global financial system. The financial impact of a pandemic is difficult to predict and hence to plan for, but the losses that would result could be substantial. Banks, in

particular, will experience significant risks in the economic downturn that will follow an outbreak - not least in their exposures to travel-related industries, as was illustrated during the relatively mild outbreak of SARS in 2003. Recent analysis by a Canadian securities firm provides some insight into the potential economic impacts of a pandemic [3] and warns firms that they must ensure that their Business Continuity Plans are updated to reflect the new realities.

This paper does **NOT** consider the financial impact on banking institutions of a pandemic (though obviously planning must be driven by the need to minimize such impacts), but focuses on the BCP and Operational Risk issues that must be addressed and suggests actions that can be taken immediately to ameliorate the impacts of a pandemic.

This paper echoes the advice of medical experts and financial analysts – Don't Panic! It should be remembered that experts do not agree on how likely an avian flu pandemic actually is, and a catastrophe may be averted by the mass culling of poultry by national government agriculture departments.

However, firms should be cautioned that a pandemic is **as least as likely** as some other scenarios for which BCP plans are already in place, and that, at the very least, banking regulators will expect firms to have considered the potential for losses as part of their economic capital regimes [4].

Basel II – External Events

In June 2004, the Basel Committee released the 'Revised Framework for the International Convergence of Capital Measurement and Capital Standards' [4], which contained definitive proposals on capital charges for Operational Risk under Basel II. In these proposals, the Basel committee defined operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from **external events**".

Banks applying to use the so-called Advanced Measurement Approach (AMAⁱ) for calculating operational risk capital are required to estimate their capital to a 99.9th percentile confidence interval - often referred to as anticipating a '1 in 1,000 year event'. While the likelihood of an influenza pandemic would surely fall within such a confidence interval, unfortunately there is no available historical 'loss data' upon which to base a reasonable statistical estimate. In such situations, banks are required to arrive at an estimate based on 'scenario analysis', drawing "on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses" [4].

As part of the evolution of Basel II rules, the Basel committee published a set of "sound practices" and 'principles' that all banks should use to manage operational risk [4]. In particular, principle 7 requires that all banks should "have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption". Banks are also required to "establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations".

In late 2005, the onset of an avian flu pandemic is most certainly a 'plausible scenario' that requires serious consideration by regulators and regulated financial institutions.

ⁱ It is highly probable that those smaller banks not required to adopt the most sophisticated AMA approach, will be forced by their national banking regulators to anticipate, and allocate economic capital for, significant losses as a result of a pandemic. Major banks will have a higher hurdle to jump.

A Framework for Pandemic Planning

No one knows precisely how a pandemic might unfold. However, the three flu pandemics of the 20th centuryⁱ give some clues as to what might be expected. The diagram below shows a *rough* timeline of how a pandemic might evolve and impact financial institutions. The known ‘facts’ used to construct the framework below are:

- The WHO defines six stages of pandemic preparedness planning [1]. In late 2005, the world is in the “Pandemic Alert Period” somewhere between stages 3 & 4, with transmission of H5N1 to humans and resulting death in several Asian countries. The lead-time between the final ‘pre-pandemic’ stage 5 [multiple, but still localised, infections] and stage 6 [a full blown global pandemic] is not known but could be as short as 2/3 months. Health authorities around the world are working hard to avert the progression to level 5 by imposing quarantine restrictions on infected families and culling domestic poultry and migrating wildfowl.
- In addition to local quarantine measures, the first line of defence in preventing human-to-human transmission is the use of anti-viral drugs [such as Tamiflu®]. Note these drugs do not cure the infection but inhibit its spread. While health authorities are frantically stockpiling these drugs, it is probable, given existing production capacity, that sufficient doses will only be available to protect essential services, such as medical staff and police.
- Until human-to-human transmission of the flu actually occurs, it will be difficult to develop a vaccine that will target the new mutated strain of the virus, although ‘general’ flu vaccines may be of some help. Experts believe that it will be at least six months after its onset until sufficient stocks of an effective vaccine are produced to slow the spread of the disease. Until an effective vaccine is developed, produced and delivered, the most effective containment mechanism will be self- (or even mandatory) quarantine. People will stay, or be forced to stay at home as schools, hospitals, retirement homes and entertainment venues are closed and public transportation is curtailed.
- Worryingly, the virus may mutate as it spreads and, as in the 1918 Spanish pandemic, create a second (or even third) wave of infection thus prolonging the disruption to the global economy. Ominously, as experienced in the Spanish flu pandemic, it cannot be assumed that, as with the annual flu epidemic, the virus will target the elderly and sick – all ages will be at risk!

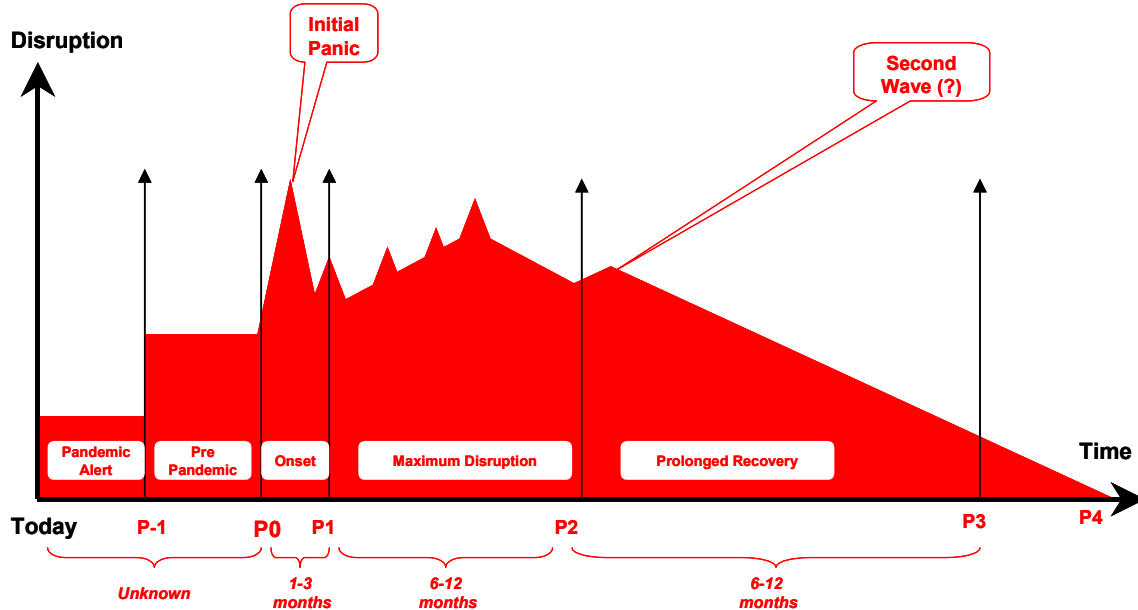


Figure 1 – Pandemic Timeline and Planning Framework

ⁱ The highly destructive ‘Spanish flu’ outbreak of 1918-19, the ‘Asian flu’ of 1957-58 and the ‘Hong Kong flu’ of 1968-69 all caused death and economic disruption on a massive scale. The relatively milder outbreak of SARS (Sudden Acute Respiratory Syndrome), a bird related disease, in 2003, in which over 750 people died worldwide, caused severe disruption in the travel and tourist industries [3].

There are five distinct ‘phases’ in the planning framework described above:

1. **Pandemic Alert** – governments are put on notice that a pandemic is possible and that preparedness plans should be reviewed and updated where necessary. At this stage, *as today*, individual firms become increasingly aware of the threats and should consider the potential negative impacts of such an event.
2. **Pre-Pandemic (WHO level 5, shown as P -1)** – localised outbreaks of the disease occur with human-to-human transmission. Government (and firms) begin to assign *specific* resources to address the heightened threat level and prepare contingency communications for the general public and staff.
3. **Pandemic Outbreak (WHO level 6, shown as P0ⁱ)** – general outbreaks of the disease with human-to-human transmission across borders. At this stage, governments (and firms) would activate *pre-planned measures*, such as border and travel restrictions, to minimize the spread of the disease. And, key emergency staff would be provided with anti-viral drugs and any general vaccines that are available.
Despite copious warnings in the ‘pre pandemic’ stage, there will inevitably be a panic in the general public at the time where a pandemic is declared, in each country. Overreaction will be inevitable as people and companies come to terms with the implications of such a deadly disease. At this stage, planners must ensure that they too don’t overreact but activate their pre-prepared plans in reaction to the reality as opposed to the hype of the situation.
4. **Maximum Disruption Period (P1-P2)**– after a, hopefully short, period of panic, the reality of the pandemic will hit home as the virus spreads, and as each country and region is affected. Outbreaks, and accompanying minor panics, will occur simultaneously and unpredictably across the world. It is in this phase, that maximum disruption to business will occur and, as the timeline shows, disruption could last for several months, depending on the virulence of the virus.
5. **Prolonged Recovery (P2-P4)** – recovery from a pandemic will be slow. The inevitable slowdown to the underlying economy will lag the disease’s Onset by several months as the pandemic impacts various industrial sectors at different times. Individual firms will have to adapt to the reality of altered business conditions and must do so while clearing unavoidable backlogs. In practice, some firms may never return to pre-pandemic normality but settle for a long period of decreased activity.

Though an inadequate analogy, management should think of the disruption illustrated in this timeline as similar to that caused by severe weather events (snowstorms, floods, hurricanes etc.) but lasting for 12-18 months! Even the best-prepared firm must also recognise that their customers and suppliers make take even longer to recover – *if at all?*

For an individual firm, the questions raised by the timeline above are:

1. What is the maximum impact of the potential disruption?
2. And, how much time could elapse between ‘Onset’ and ‘Recovery’ (i.e. P0-P4)?

Unfortunately, it is not possible to answer such questions given our limited experience of the speed of virus transmission in the modern highly inter-connected world and without considering the individual circumstances of each firm.

Even in an extreme pandemic some firms will, mainly by good fortune, remain relatively unscathed as the virus hits their region late, or not at all. Conversely, even well prepared firms may suffer enormous disruption if they are hit early before effective containment procedures are in place.

It is obvious however that, even if relatively unscathed, the risk of disruption will not diminish quickly. The period of ‘maximum disruption’ will last several months, being determined by the speed at which the virus spreads and the time taken to develop sufficient quantities of an effective vaccine. Nor will recovery be swift. The slow down of the

ⁱ It should be noted that events such as ‘Outbreak’ (shown as P0) will not be instantaneous points in time but may occur over several weeks, as false alarms and rumours confuse the real picture. In reality, it will only be after an event that hindsight will show definitively when a pandemic starts and finishes.

general economy, the need to clear any back-logs that have built up while business is disrupted and the unsettling task of training new staff to fill the shoes of those who unfortunately succumbed to the virus, will take some time.

It is worth noting, however, that large firms with geographically dispersed offices, and critical operations centralised across businesses **are most at risk**. Such firms are likely to be hit simultaneously in multiple locations with one or more of their central functions being severely disrupted. For example, a global bank with offices in all major financial centres, and back-office operations outsourced to populous centres such as India, can expect maximum disruption, as business in one country cannot be conducted because of interruption to operations in other countries.

At this point it is worth remembering that the onset of a global avian flu pandemic is far from certain! Any analysis of the potential impact of a pandemic must be (a) to anticipate the measures needed to protect staff and customers and (b) to ensure that firms are as well positioned as possible to ride out inevitable disruptions.

Business Continuity Planning

Since the events of September 11th 2001- and the non-event of Y2K - Business Continuity Planning has been predominantly based upon reacting to, and recovering quickly from, a sudden and catastrophic loss of premises or computer systems. The high-level BCP strategy for most firms in the banking industry is to operate with 'spare' infrastructure in several geographically dispersed locations. In the event of losing access to one location, staff or systems would normally be relocated to unaffected locations and be 'crammed' into the premises that remain operational.

This is precisely the **WRONG** strategy for dealing with a pandemic where overcrowding would be considered dangerous and strongly discouraged by civil authorities. In a pandemic, premises and systems will largely be unaffected; **it is the people who use them who will be unavailable!**

The initial response of civil authorities to an outbreak will be to discourage large gatherings of people. The crowded call centres and dealing rooms of modern financial institutions will be ideal places for infection to spread, and it would be prudent, for planning purposes, to assume that the number of staff permitted in such crowded spaces would be curtailed, potentially for several weeks or months.

As an example, retail banks will have difficulty coping if – as long hoped for - customers abandon queues in branches, turning instead to call centres which have been staffed with an increasingly casualized, predominantly female, often outsourced workforce. Many of these casual workers will find it difficult to turn up for work, having to care instead for children sent home from school and elderly relatives displaced from crowded hospitals and nursing homes. At the same time, call volumes will rise, as customers feel the need to increase their (already elevated) credit card limits to cope with medical costs and lost wages. More work, fewer people - is a recipe for operational disaster.

Insurance companies face a particularly nasty 'triple whammy': not only will claims rise, as death and disability increase; at the same time business will pick up as people take out, or increase, their life insurance policies; but, as a result of the pandemic, fewer staff will be available to cope with the increased volume of business. Problems will be compounded if the banks, upon which they depend, cannot cope with the increased premium and claims payments.

Business continuity planning assumptions to cope with a pandemic are very different to those used in infrastructure 'Disaster Recovery' planning scenarios.

Where existing BCP planning does anticipate loss of access to staff rather than premises, as for example in a transportation strike, the underlying assumption is often that such disruptions will be short-lived, measured in days rather than weeks or months. Planning for such events often involves putting staff up in local hotels and sometimes on camp beds in offices – a solution that would not be feasible for a prolonged disruption. In these circumstances, the option of working from home is often promoted but again it is assumed that this would be for a relatively short term – little organizational or technical infrastructure is put in place to support long-term working from home.

For BCP planning purposes, it would be prudent to make the following high-level planning assumptions:

1. The impact of a pandemic, if one were to break out, would be unpredictable; any business location could be affected and multiple offices could be impacted at the same time.

2. Civil authorities, *and sensible management*, will wish to limit human-to-human transmission of the disease and therefore will discourage, even medium sized, gatherings of people.
3. Provided that the continued operation of key infrastructure (data centres, networks and systems) is accorded highest priority, the major problem then becomes one of managing people resourcesⁱ. While all numbers are mere guesstimates, medical experts have projected that, in a full-scale pandemic, 25% of people will contract the virus, but a much higher percentage will be indirectly impacted, for example staying away from work to care for family members. For planning purposes, the figure of 25% absenteeism should be taken as a “low estimate” for medium term disruption, increasing in larger cities to 50% or more for short periods.
4. In the event of a pandemic, business will not return to normality for a period of 6 – 18 months; on the low side if the pandemic proves to be relatively benign and is handled effectively by national governments; on the high side if major financial centres are, even moderately, impacted. A working assumption of severe disruption lasting 12 months would be supportable.
5. It cannot be assumed that all outsourcing arrangements will necessarily operate at contracted service levels. One part of the world may be affected only mildly by a pandemic but nevertheless firms may be seriously disrupted by serious outbreaks of disease impacting their suppliers in other countries. Overall, it is those firms that have created highly automated, ‘just in time’ value chains, outsourcing core activities to third parties, that will be most at risk.

Organizing for a Pandemic

Paradoxically, it is those firms at the extreme ends of the organizational ‘culture’ spectrum that will be most at risk from the (temporary or permanent) loss of staff during a pandemic. It is easy to see that a firm with a strict, hierarchical, “command and control” culture is at risk if one or more of its key decision makers (“generals”) were to become incapacitated. At the other extreme, organizations that are ‘consensus driven’ will also have difficulty making consensual decisions if key participants are not available to take part in every debateⁱⁱ.

The firms most able to survive in a situation where key staff may become unavailable for prolonged periods are those where decision-making is devolved to semi-autonomous business units *at all levels of the organization*. In the language of war, it is small, flexible self-managed ‘guerrilla cell’ or ‘special forces units’ that are able to survive in the face of seemingly overwhelming odds.

The key organizational qualities of such ‘cells’, is that, once allocated to a *well-defined* task, they are largely autonomous, solving problems and making day to day decisions largely within the group itself and communicating progress to higher level command only when needed. Organization within such ‘cells’ is not rigidly hierarchical and information is shared freely so that the group as a whole is not endangered by the loss of a key member. While there are specializations within such groups, members are trained in more than one skill so that gaps can be plugged if they open up. A critical skill is communication; clear and reliable flows of information (using trusted ‘couriers’) are essential to any organization facing adversity. Interestingly, this flexible, semi-autonomous model of organization is similar to that of the Internet, which was originally designed to withstand the loss of multiple components in a nuclear attack, continuing to communicate using whatever resources were still available. The architecture of the Internet provides some clues as to how to mitigate the impact of the disruption caused by a widespread pandemic.

It is unrealistic, however, to presume that any organization would change a long-established and successful culture in reaction to a threat that is still prospective rather than real. On the other hand, it would be dangerous for planners to assume that there are no weaknesses in a firm’s organization that may prove problematic in the face of a new threat. It is important that BCP planners recognise such potential weaknesses and plan strategies that will mitigate them.

ⁱ Note that the equally important problem of managing financial assets is not addressed in this paper.

ⁱⁱ Firms with an excessive ‘meeting culture’ should be particularly alert to the problems that might occur if decision-making meetings were to be curtailed for a period.

Planning Strategies for Tackling a Flu Pandemic

The three key questions that must be answered by any strategies for tackling a flu pandemic in an individual firm are:

1. How can the firm continue to operate effectively with minimal contact between staff and between staff and customers and suppliers for prolonged periods?
2. How can the firm continue to operate effectively if key staff are incapacitated for prolonged periods, or even permanently?
3. How can the firm continue to operate effectively if their 'value/supply chains' are disrupted?

The overall strategy for addressing Question 1 (minimizing contact) boils down to promoting working at home - 'telecommuting' in IT jargon. The overall strategies for addressing Question 2 (Loss of Key Staff) are (a) to encourage autonomous decision-making within 'focused business cells' and (b) to encourage maximum communication between members of such cells. Question 3 (value chain disruption) is the most difficult to answer and, because time and cost preclude creating new value chain links prior to the onset of a pandemic, the ultimate strategy (as in manufacturing industries) will be to curtail or even shut down the operations effected.

Civil authorities, and prudent management will encourage staff to work at home. However, technology will be required to allow them to do so effectively. Firms will have to consider seriously the costs of providing high-speed, high capacity technology for their staff to work at home – few home PCs will have the horsepower to cope with the workload involved¹. However, modern off-the-shelf technologies such as Broadband Internet, Email, PDF formatted reports, VOIP (Voice Over IP) telephony, web logs (blogs), instant messaging and mobile phones, make it possible for staff working alone, or organized into small 'focused business cells', to continue to operate, albeit in a degraded capacity, even though operating remotely from each other.

In practical terms, while firms will have some time to respond to warnings of an impending pandemic, they will not have sufficient time to react from a standing start. As effective remote communication will be critical to mitigating disruptions, firms should encourage their staff to install Broadband Internet access at home, with appropriate financial incentives to do so. Staff should also be encouraged to work at home intermittently to test the technology and their ability to communicate effectively with their co-workers and to access operational information effectively.

Managers and staff on the front line of a business are usually best placed to fix even serious problems as they arise. What stops them doing so are often-unnecessary constraints placed upon them by upper-level management. Constant referral of decisions up the chain of command or unnecessary review of lower level decision-making generates reliance on a hierarchical management structure that could prove risky in a pandemic. Operational executives should consider the limits and responsibilities of the units that they manage and, to promote decision-making autonomy within these units, practice sending decisions back to staff for local resolution, and reward staff for doing so.

¹ As many firms already supply such technology to mobile staff, the issue then becomes one of the making the additional investments needed to provide the technology to a larger proportion of the workforce. A moment's consideration will show that such investments will be paid back rapidly if staff are forced to stay at home for prolonged periods yet are enabled to continue to work effectively. In budgeting terms, this is merely bringing forward expenditure from future years rather than making totally new investments.

Practical first steps in developing a Pandemic Plan

The following *first steps* are suggested for ‘jump-starting’ the development of a business continuity plan designed to mitigate the impact of an Avian Flu Pandemic.

Corporate Governance

It is suggested that firms (if they have not already done so):

- Immediately, set up a Pandemic Planning and Coordination Unit (PPCU) within the Operational Risk Management department as part of the existing BCP function.
- Staff the unit with at least the following skills:
 - Medical expertise to provide independent, objective information on the background, status and potential trajectory of a pandemic, possibly using part time experts from university medical departments. Note additional medical safety measures, such as making facemasks available, will also be needed.
 - Communications expertise to develop material for distribution to customers and staff;
 - Information experts to develop and operate public/private web sites and firm-wide communications capabilities, such as email and ‘web-logs’.
 - Telecommunications experts who would ensure efficient secure, access to corporate information by remote staff and who would develop and promote the effective use of voice and video-conferencing.
 - Security experts who would ensure that premises and the staff remaining in them are secured and who would liaise with civil authorities to ensure compliance with changing ordinances.
- Identify and assign senior executive responsibilities for initially overseeing and, should the need arise, taking control of the Pandemic Planning and Coordination activities
- Immediately, raise the issue of Pandemic Planning to the Risk Committee of the Board for detailed oversight and place the issue on the agenda of *every* Board meeting going forward.
- Run an education workshop for the Board and senior management to explain the risks and to discuss options for mitigating these risks.
- With direction from the Board and senior management, develop policies for operating in a Pandemic. Such policies might include: priorities for reducing risks and slowing down businesses; changes to delegated authorities; changes to staff entitlements and remuneration; and so on.
- As a demonstration of senior management’s commitment to competent BCP planning and to ensure that supporting technology is working satisfactorily:
 - Hold a number of up-coming Board meetings *completely by teleconference*, i.e. with all board members participating from home.
 - For each Executive Committee meeting going forward, ensure that one or more of the members participate from home.

Identification of Key Risks

Identification of Key Risks should concentrate on the four areas of operational risk identified in Basel II, i.e. ‘processes, people, systems and external events’:

1. **People and Organization Risks** – a ‘map’ of the entire organization should be developed that shows not merely key responsibilities but also the linkages and dependences between business functions. For each function a list of key roles and individuals holding (or capable of holding) those roles should be developed. For each function also, the degree of ‘operational autonomy’ should be evaluated. The goal of such a map would be to identify potential ‘**key people**’ risks in the current organization and to highlight where mitigating actions, such as staff transfers and increased decision-making delegation would be beneficial.
2. **Process Risk** – a map of all major ‘end-to-end processes’ in the organization should be developed that shows not merely key operations performed in each process but also potential bottlenecks and critical internal and external dependencies. The goal of such a map would be to identify potential “**key process**” risks in ‘core’ processes, such as where increased volumes might overwhelm current, never mind depleted, resources and to highlight where mitigating actions, such as increased automation, would be beneficial.

3. **Systems Risks** – a map of all major systems in the organization should be developed that shows not merely key technical attributes but also dependencies on human intervention, including data centre operations. The goal of such a map would be to identify potential “**key systems**” risks, such as where a large degree of human intervention is needed to access information to operate the business and to highlight where mitigating actions, such as increased electronic report production, would be beneficial.
4. **Telecommunications** – a ‘map’ of the entire telecommunications network supporting the organization should be developed that shows not merely the network topology but also capacity bottlenecks within the network. The goal of such a map would be to identify potential “**key systems**” risks in the current telecommunications infrastructure and to highlight where mitigating actions, such as increasing capacity, would be beneficial.
5. **Value Chain¹ and Outsourcing** – all outsourcing and value chain dependencies across the organization should be evaluated from an operational risk perspective, considering: (a) contractual agreements; (b) current performance; (c) problems with current performance; (d) vulnerability of the outsourcer to disruption; and (e) vulnerability of the firm to non-performance by the outsourcer [4]. The goal of such a review would be to identify potential “**key external**” risks in current outsourcing arrangements and to highlight where mitigating actions, such as reduction in dependency, would be beneficial.

Communication

As a matter of priority, material for communicating to staff and customers information about the firm’s response to a pandemic should be developed:

1. Policies for the content and delivery of external and internal communications on all matters relating to the impact of the pandemic should be developed, as a matter of urgency;
2. Specific material for staff should be developed that describes not only how businesses should operate in reduced circumstances but also provides information for handling personal issues (e.g. sick relatives).
3. Specific material for customers, including guides to using electronic services (ATM, Online Banking, Call Centres etc.). It should also be recognised that existing communication material may be overtaken by events, such as alterations to terms and conditions on lending and credit card products and changes to customer contact numbers.

Telecommunication

Effective telecommunications will be critical to minimizing the potential disruption resulting from a pandemic. It is suggested that the following issues should be addressed as a matter of priority:

1. **IVR**– Interactive Voice Response (IVR) is the technology that initially answers customers’ telephone calls and, after requesting some pertinent information, attempts to route the call to an available operator. This technology will be critical to effective operations in a pandemic, since not only will the volume of calls increase as customers telephone, rather than visit, their banks but call centre staff will be dispersed to new locations. The following actions should be prioritised:
 - Determine the peak capacity of the current IVR network and develop an upgrade plan for adding capacity.
 - Ensure sufficient IVR ‘scripting’ capabilities are available and hire additional staff if required. Staff will not only be required to change messages on ‘scripts’ as the pandemic communication plan evolves but will also be required to develop new capabilities, such as accessing additional customer information.
 - Develop, if not already available, capabilities for switching customer calls to external telephones, such as to staff in unaffected offices or working at home.
 - Develop, if not already available, capabilities for recording customer calls and making them available to remote staff for action.
2. **Web Site** – Internet traffic will inevitably increase (potentially many times over) in the event of a pandemic as customers begin to work from home and businesses move to performing their banking on-line. This will place considerable strain on all aspects of a firm’s web-site capabilities not merely as a result of increased volumes but also the need to provide additional information on-line. Experts will be required to implement all of the changes to a firm’s web sites that will be required, but it should be noted that hiring competent experts might prove difficult, even before the onset of a pandemic.

¹ While not technically outsourcers, agencies such as clearing houses and information providers are critical to the effective operation of the value chain most banks.

3. **Telecommuting** – Staff will be encouraged to work from home for long periods in the event of a pandemic. While telecommuting has been actively promoted for several years, it has rarely become the primary mode of working for business professionals. There are several major problems that must be overcome before staff can work effectively away from their normal office. But technical solutions do exist to overcome most of these problems:
- Computing capabilities – staff need appropriate computer capabilities at their fingertips. In practice, this means supplying staff with capabilities almost identical to that used at their desks. The best solution to this problem is to provide staff with a fully configured portable PC that can be carried easily between home and office [in extreme cases, a desktop PC could also be moved]. Firms must decide when to invest in these capabilities, and should do so well ahead of time to ensure that the technology will work when required.
 - Internet Access – to operate effectively at home staff need access to the Internet. While dial up connections can be used, connection via broadband will provide access to the increased amount of information that staff will need. Firms must consider the cost of providing such services in bulk for staff working remotely and must do so well in advance of when such a connection may be needed.
 - Telephone Access – to operate effectively at home, staff will need to be able to make and receive unrestricted telephone calls. While the home or even mobile phone can be used, prolonged operation from home will inevitably require a dedicated telephone. With Broadband access to the Internet, VOIP technology can be used to provide such a service. Firms should seriously consider the cost of providing an open VOIP capability and connecting that capability to its internal telephone networks, for example for telephone conferencing between staff.
 - Application Access – by far the biggest hurdle to home working will be providing staff working at home with access to internal applications. While some software, such as Email may be relatively easy to open up to access from home, other older applications may prove more difficult. Where firms have not already done so, use of technologies such as ‘terminal emulation’ and ‘thin client’ over the Internet will have to be investigated, and implemented as a matter of urgency.
 - Information Access – staff will need access to relevant business information to do their job but often the information that is available is not suitable for home working. For example, it will not be feasible to deliver large volumes of computer-generated printout to all staff who may need it. Where firms have not already done so, information will have to be made available to staff on-line (such as in Adobe® PDF format). It should be noted however that merely providing a file will not be sufficient as printing on a home printer, however fast, would not be feasible. Software for splitting, indexing and searching information will have to be investigated and implemented ahead of time.

The suggested ‘first steps’ listed above merely scratch the surface of what would be needed to deal effectively with an Avian Flu Pandemic. What the suggested actions do show, however, is that there is a considerable lead-time in implementing some of the solutions necessary to tackle the disruptions that would occur. And, even before any actions can be started, the planning process itself must be fired up and must gain management commitment and funding.

Given the increasing emphasis being placed on the potential for severe disruption resulting from a pandemic, firms should ask themselves whether they should already have started developing an appropriate BCP!

Summary

This paper argues that Business Continuity Planning for mitigating the impact of an Avian Flu Pandemic is, very, different to the planning required to cope with the loss of key infrastructure. Underlying assumptions are different, as are mitigation strategies.

While a global pandemic is far from certain, its onset is sufficiently likely that financial institutions should seriously consider the potential impacts on their businesses. If an outbreak were to occur disruption could be very serious, particularly to those firms with worldwide offices and/or highly centralised operations.

This paper attempts to ‘jump start’ debate on the subject of BCP planning for a pandemic, in the context of Operational Risk Management, in particular the need to anticipate the economic losses that could occur as a result of such an ‘external event’ as required under Basel II.

The paper develops a framework for developing plans to help mitigate the impacts of such a disaster and identifies some key questions that must be answered when developing such a plan. Much work needs to be done to put in place robust plans for coping with a pandemic, and it can only be hoped that the work will never be needed.

Finally, it is worth yet again repeating the advice of experts – Don't Panic! Firms will be better served by coolly analysing the potential impacts of *any* potential disaster, before its onset, than by overreacting if such an event were to occur. That is the business rationale for Operational Risk Management and Business Continuity Planning.

References

- [1] For general background on the history and information on the current status, of Avian Flu and on medical preparedness planning for a pandemic see the web-sites of the World health Organization (WHO) www.who.int and the Centre for Disease Control (CDC) www.cdc.gov/flu. Many national health authorities also have information on the state of pandemic preparedness within their jurisdictions on their web sites, e.g. www.dh.gov.uk/pandemicflu. See also the special Avian Flu web sites on Nature www.nature.com and the Royal Institute of Science www.risci.org
- [2] For good descriptions of the pathology of the avian flu virus H5N1, see Nature (2005) "Special Edition on Avian Flu". May and Osterholm M.T. (2005) "Preparing for the next Pandemic", New England Journal of Medicine May www.nejm.org
- [3] For analyses of the potential economic impact of an Avian Flu Pandemic see Cooper & Coxe (2005) "An Investor's Guide to Avian Flu" August and "Don't Fear Fear", October; BMO Nesbitt Burns www.bmonesbittburns.com
- [4] Basel II regulations were formalised by the Bank For international Settlements (BIS) in "International Convergence of Capital Measurement and Capital Standards - A Revised Framework" June 2004 and a set of risk management principles, including BCP, in "Sound Practices for the Management and Supervision of Operational Risk" February 2003. Sound principles for managing the risks in outsourcing arrangements are also developed in "Outsourcing in Financial Services" February 2005. All BIS documents are available on-line at www.bis.org.

DR. PATRICK MC CONNELL is a partner at Risk Trading Technology, a small consultancy specializing in operational risk management and information technology. He is a Visiting Fellow at the Macquarie University Applied Finance Centre, Sydney, where he teaches a course on Managing Operational Risk and can be reached at pjmconnell@computer.org.