CRMG
CYBER RISK MANAGEMENT GROUP

*Thank you for attending the '**Shifting cybersecurity from a compliance to a risk focus**' webinar by CRMG and Galvanize. Below are questions from the audience that were unable to be answered due to time running out. CRMG's Nick Frost (Co-Founder & Director) has provided detailed answers.*

*We hope this is helpful, and for any further questions please contact us at **info@crmg-consult.com**.*

Questions

1. There is plenty of regulation (and positioning by Audit, CISO, ERM, etc.) around taking a risk-based approach, but little actionable help on conducting a reliable and repeatable risk assessment, so, how can CRMG and Galvanize help here?

That's a good point in the majority of cases, although regulations are starting to be prescriptive in their expectations as to what a risk-based approach must entail (and there is a very small number emerging) such as the NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES Cyber Security Requirements for Financial Services Companies https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

Whilst there are many regulations and examples of legislation that refer to the need for a risk-based approach, there is a need to explicitly clarify what the expectations are here (i.e. follow an industry recognised methodology, consistent use of threat, control and impact libraries etc).

Where we will see specific details regarding a risk-based approach will be in the Financial Sector as regulators are genuinely concerned about bank stability and the disproportionate impact a major cyber-attack could have on a bank (and the systemic impacts this would have on operations, loss of customers, and so on).

The specific areas in which CRMG can help are as follows:

1. **Identify your organisations legal and regulatory landscape for cybersecurity;** CRMG will work with your legal team and conduct an assessment of the legal and regulatory landscape for your organisation
2. **Interpret the legal and regulatory requirements in cybersecurity for your business;** CRMG will work with the legal and security team to translate what the legal and or regulatory text means in practice so that there is no ambiguity and no duplication due to overlaps with the mandated requirements – basically we keep it simple but aligned
3. **Compare and contrast your cybersecurity strategy to the legal and regulatory landscape;** CRMG will set out areas in your organisations cybersecurity strategy that we believe should be enhanced to align to the legal and regulatory landscape, i.e. areas that could be misinterpreted by a regulator or auditor, areas that may require a mapping that demonstrates the alignment of the strategy to the specific pieces of legal/regulatory mandates.

CRMG has a lot of experience in this area and we have members of our team that have held global roles in cybersecurity for FORTUNE 500 companies that have worked specifically in this area to help map these mandates and interpret them for the business and security function they worked for. Galvanize also have a range of content that can support alignment to many of these legal and regulatory mandates such as GDPR.

2. Is the risk-based approach about agility in responding to what is on the mind of business leader's vs ticking a box for regulators?

My honest view would be to focus on what is on the mind of the business as it (the business) would be keen to square away the regulators anyway and will consider this in their decision-making about where to focus a cyber risk programme. The only real way to achieve this is by working closely with the business.

Agile is a key word here, and I'm glad you mentioned it as the business may have a need to conduct risk assessments that cover a number of situations – many of which we wouldn't have seen at CRMG a few years ago. These include scenarios such as:

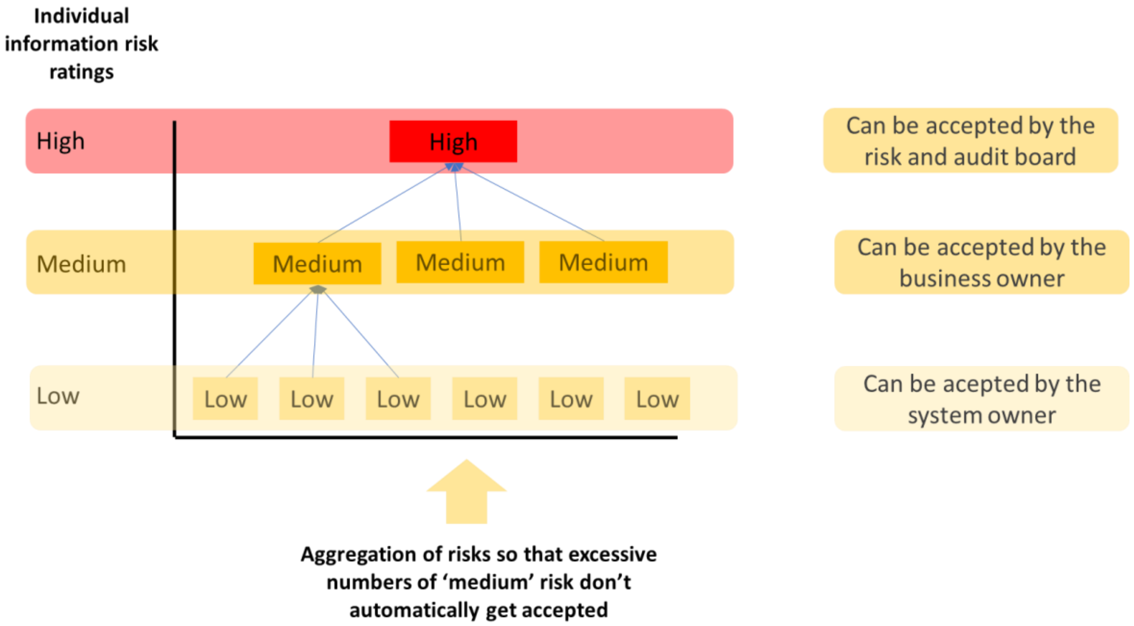
- We are looking to acquire a company and part of our due diligence requires a cyber risk assessment/profile so that mitigating actions are taken prior to completion of the transaction. Can you complete this in a month?
- The organisation is looking to float on a stock market; we have a Chief Commercial Officer joining this week to manage this process. They have asked for a cyber risk assessment of our critical systems as we need to demonstrate our understanding of the cyber risk landscape and align our cyber strategy to this
- As a Private equity firm, we are looking to invest in a Series B round for one of our clients. It's a significant investment and before we go ahead, we need to engage you in carrying out an independent risk assessment of the company.

Then there are the mainstay reasons for conducting risk assessments, such as:

- Targeting and validating your need for budget. An analogy I sometimes use is that of a doctor giving you a prescription without diagnosing the ailment
- Regulatory requirement. Regulators are becoming more focused on the need for risk assessments to pave the way for determining your strategy and minimizing impact
- Using risk assessment outputs to validate change or support existing direction in key areas of your cyber programme such as:
    - Scenario planning: running scenarios that align with your key risks
    - Targeting the awareness messages for staff to key risks that they can influence. Utilisation of staff time to attend awareness training (online or classroom-based) is revenue lost (in the eyes of the business), so targeting that time to areas of risk that are key to the business is necessary
    - Monitoring threats that can cause the risks – through your security ops centre (or equivalent). If this is managed by an outsourced service provider they are likely to go with what they believe are the threats to your organisation (which might be applicable), but a blended approach of 'What they are seeing in your industry sector' and 'What you have defined as the prioritised risks' is a better way to handle this.

3. For Accepting Risk, doesn't it really have to be a formalized process and accepted by the right party? Poor risk governance can ruin the risk decision process.

Yes, I believe that it does need to be formalized. You could end up in a tricky situation if a breach occurs (e.g. an insider sells vast amounts of PAN data or PII on the dark web) and this risk has been accepted with little to no governance or escalation activities to validate such a decision. The idea of governance and escalation procedures are not aimed at slowing down the risk response process (i.e. do we mitigate, or do we accept?). They will to a degree, BUT, the idea is that accepting a high level of risks needs to be discussed by a committee within the business. The other point to be aware of is that the business may agree to mitigate a 'High' risk but accept 'Medium' risks. If the system has multiple medium risks and the aggregated effect is a High/critical, risk what should the organisation do then? Here is an idea we suggested for a client; it's nothing new and is used in auditing a lot, but it helped respond to the client's needs:


Individual information risk ratings
High
High
Medium
Medium
Medium
Medium
Low
Low
Low
Low
Low
Low
Low
Can be accepted by the risk and audit board
Can be accepted by the business owner
Can be accepted by the system owner
Aggregation of risks so that excessive numbers of 'medium' risk don't automatically get accepted

4. If available, can you please point us to a web link on risk appetite statement? It varies between organization/industry; I just want to see examples out there.

Sure. Here are a few good general sources I have used in the past.

This is a good report; it's 2 years old now but still applicable. Review pages 15 and 16.
https://www.nao.org.uk/wp-content/uploads/2019/05/Good-practice-in-annual-reports-2107-2018.pdf

This is from COSO which is broader and aimed at Enterprise risk, but still applicable as we should – in cyber risk – align our risks with the corporate risk appetite statement, despite how vague it might appear.
https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

Another one that I find very well defined can be found in an annual report. The latest annual report (as I recall) also has the same level of detail as this 2017 version.
https://www.annualreport2017.weir/documents/Risk%20Review.pdf

You are correct in that risk appetite is still more of an art than a science. It is often ignored in my experience, as it is seen to be difficult in practice to apply or work with. However, this is no reason for ignoring it.

5. What about benchmarking? We often get asked: "how am I doing against my peers?"

I have always been a supporter of any benchmarking activity in information security. It's a hugely powerful project for security functions – so long as it's carried out in a transparent and objective manner, AND with sufficient comparison data. Where I find security benchmarking to be of most value is in helping to compare against industry control trends, not necessarily following an industry standard which can be high-level and poorly aligned with specific sectors.

Risk professionals often ask for the next level of detail, for example “What are my peers doing on Access Controls?” or “To what extent are Business Impact Assessments conducted as part of a broader risk assessment capability?”. These are questions that benchmarking can assist with.

There are many benchmarking services out there and the ones I know of anonymise the data, so you can see your results vs those in your sector - and vice versa - for other organisations taking part. My experience implementing a benchmarking capability was that it was of great interest to senior management as it can polarize the response to questions such as “Why are we lower than our peers here?” or “Are we spending too much here as we are way above anyone else?”. The point is that these questions from senior management are what you need to create a dialogue with the business around introducing changes and explaining the reason why you are not the top Bar in the chart. A key question I would ask any benchmarking provider is “How many organisations in my sector have contributed to the benchmarking over the past 2 years?”. You need to get specifics to ensure that the data set you are comparing yourself against is large and current.

6. Can you talk about "Mitigate Risk Cost factor" assessment techniques?

This is often the ultimate question to answer in order to convince the organisation that mitigating a risk (taking into account its cost) is a logical way forward. The two key components to help inform the response here is:

- What is the cost to the business if we are impacted by this risk?
- What is the cost of implementing the control to mitigate this risk?

There are two approaches that you can take to providing a financial figure to answer these questions. 1) Make a subjective decision (based on factors to consider below) or 2) apply the factors below to a quantitative / statistical approach.

- What is the cost to the business if we are impacted by this risk?
    - Consider factors such as; *Regulatory penalties, Investment in the marketing/business development required to restore reputational damage, Cost set aside for 3rd party experts to clean up the aftermath of the attack (e.g. Ransomware on laptops), Cost associated with unforeseen activities (e.g. management spending more time on addressing the issue and restoring faith amongst key clients)*
- What is the cost of implementing the control to mitigate this risk?
    - Consider factors such as CAPEX spend (e.g. solutions to acquire and implement by a 3rd party), OPEX spend (e.g. training staff to operate the technology solution).

It is a worthwhile exercise to go through and you wont get it 100% correct, but you are making judgements based on a level of rigour which better informs the business as to the balance between the cost of a risk/impact to the business and the cost of implementing a control(s).

7. A McKinsey study revealed that 60% of CIOs avoided cyber security governance improvements because agility and innovation could be slowed down by 'slow security'. In other words, they accepted higher security risks as a trade-off for agility. What are your thoughts on this?

I completely agree with this finding. It is one of the reasons why I see the reporting line changing from the CIO to other C-level roles such as CRO, Head of Legal or COO. Cyber risk is a business issue and not an IT issue. From a CIO perspective I also get why they would be willing to accept higher levels of risk, as they are ultimately are judged on IT delivery first, and then secure solutions second, third, fourth…

In my experience working with clients, the level of security assessment and risk assessment is typically dictated by the time to deliver a technology/project. There are a few options that can help here, but none are silver bullets:

1. Establish a triage approach; assess risk so that time is spent on the most critical systems. Such an approach helps to 'pick the battles' to fight. It is also predicated on good business sense as we can't apply the level of rigour we want to in security to **all** systems, but we can make noises about those systems that are classed as 'crown jewels' to the business
2. Establish a steering committee; so that the decision as to whether to accept / mitigate risk is not decided by the CIO but a broader business group. Now, if you are reporting to the CIO this will not be an easy sell and may make you *persona non grata*, so you may want to look at option 3
3. Develop a 'lite' approach for security and risk assessments; Many approaches are heavy and require staff utilization from other parts of the business – which adds considerable value but increases elapsed time and ultimately can have a heavy impact on technology project delivery timelines.

If the reason for a CIO accepting high risks is down to cost, then you should focus on option 2. If the reason for a CIO accepting the high risks is down to time, then you should focus on options 1 and 3.

8. "Risk to what?" has always been forefront in my experience when creating the risk approach - "it depends" is the answer of course - there should be an industry baseline approach - does this exist?

From my perspective it is a risk to the business, but I would unpack this further, so it has more relevance from a business perspective. I have always tried to focus on what the risk looks like in terms of impact to key business characteristics such as Reputation; Loss of management controls; Legal/Regulatory penalties; Increase to competition etc.

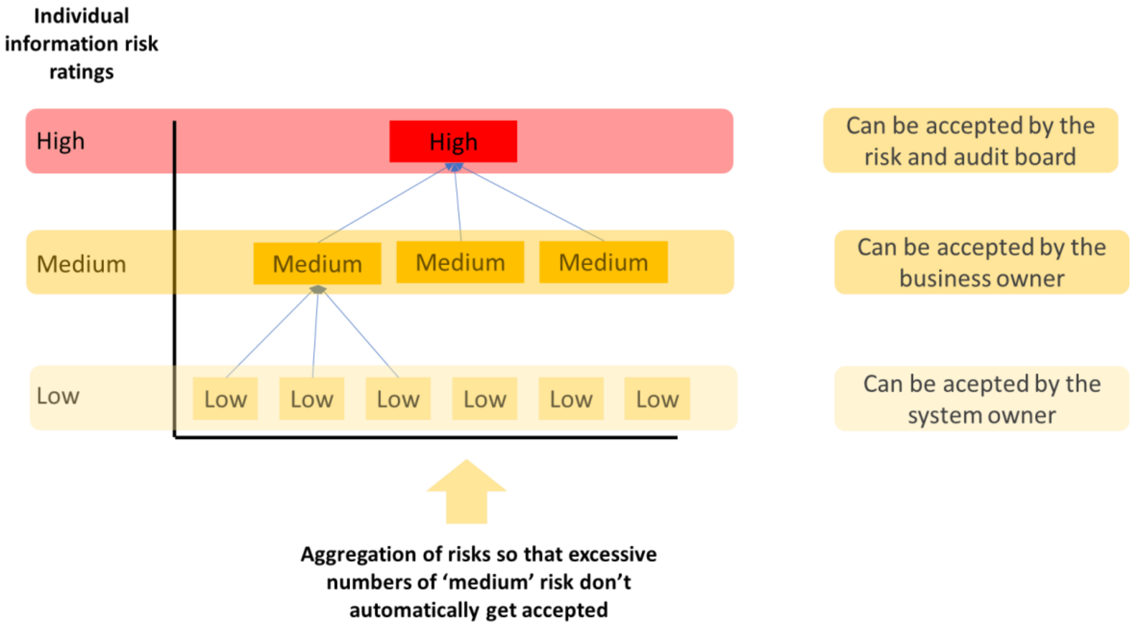
A risk or security assessment must link back to the business. Remember this is not a technical focus on the security of a protocol, or the risk from using digital certificates from provider X or Y. This is a cyber risk assessment of a key system, business process or data centre - and so there is a need to translate this risk into business language otherwise you start creating false ceilings which limit the extent to which the information can be understood.

There are baseline approaches / methodologies to risk assessment that exist, such as ISO 27005, NIST 800-37, IRAM2 (provided by the ISF). These will all reference the risk to the business.

9. What if the CIO of a government client refuses to sign-off on (accept) all risk, but asks you to take a workaround?

Well, this sounds like a tough ask. There are several options you can adopt but without understanding your organisation I don't know if this is achievable, but here you go:

1. Establish a Risk – Audit group. The idea is that the decisions for accepting risk (and risk appetite) should be taken by a broader group representing the business. This group should include the CIO, and it should ultimately listen to the CIO's rationale for accepting risk. The group should - as a committee - determine the response to the risks (mitigate/accept)
2. Introduce a model such as below to ensure that the business owners don't not just focus on addressing the '**Highs'** when there are a significant number of '**Mediums'** that (when aggregated) could result in a High risk


Individual information risk ratings
High
High
Medium
Medium
Medium
Medium
Low
Low
Low
Low
Low
Low
Low
Can be accepted by the risk and audit board
Can be accepted by the business owner
Can be acepted by the system owner
Aggregation of risks so that excessive numbers of 'medium' risk don't automatically get accepted

3. Options for mitigation. I would recommend providing 'Bronze, Silver, Gold' risk mitigation. For each one I would include the cost and the estimated level of disruption to the business so that the stakeholders have full visibility and can make a choice. They can always reject all 3 options.

10. Taking as a fact that a risk-based approach is a better way to deal with cyber security, can you give us any kind of practical advice to help our organizations transition to a risk-based approach? Steps? Stages?

I will have a go at this in the paragraph below, but if you want more details, let's organise a call.
If you have no cyber risk-based approach today, then your first step is to prove the business value. Some of my suggestions may seem obvious but they work.

Influence the business

1. Convince the business of the financial value
   a. Cyber risk assessment targets investment so that there is less of the overspend that is is common in compliance-based approaches
   b. A risk-based approach reduces the financial cost of a breach. If you have started to identify the key risk trends to the organisation e.g. *Phishing attacks from outside, Loss of sensitive data from insiders,* then you can start to plan your response to such attacks and ultimately minimize impact. Scenario planning should always be driven by the prioritised risks which are identified from conducting cyber risk assessments.
2. Demonstrates leading thinking
   a. Clients will start to expect a greater focus on cyber risks, especially the larger clients you have. So, demonstrate best practice in cyber security and emphasise the focus on cyber risk assessments in driving your decisions for controls to minimize the likelihood of a cyber-attack
   b. If you are working in a regulated environment, then this will also help convince the business.

Pilot test the approach

1. Select a practical methodology that works in your organisation
   a. Focus on ensuring that the methodology is based on assessing the key components of risk (Impact and Likelihood)
   b. Ensure that the methodology can be adapted – i.e. you can establish a 'Lite' approach for non-critical systems and a detailed approach for mission-critical systems. You need that flexibility
   c. Supported by a tool. At some point there will be a need to automate the process and to start collecting the data and outputs to determine what the key trends are
   d. Run a series of pilot assessments on systems that are well known to the business. This will drive home awareness about the possible risks and recommended actions to mitigate such risks.

Let me know if you need more assistance, as it may be worth looking at a tailored approach depending on your organisation and its level of maturity.

11. I work in the dot gov environment where NIST 800-53 etc. is gospel. I'm trying my best to bring a risk-based approach instead of a control-based approach. Now this is the government, so there's much pushback. What is your suggestion for an approach for change?

I find NIST 800-53 to be a really good source of controls, but as you will know 450+ pages of content can make implementing this quite a challenge. As your organisation will most likely follow NIST guidance, have you considered the NIST – CSF (Cyber Security Framework)? We are seeing this as the leading 'lite' approach for cyber security, especially in North America. In the document it stipulates the application of a control library as follows: *To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks.*

Your organisation may feel happier to focus on another NIST guide but one that supports a risk-based approach. As a government I don't think cost is likely to be a major issue here - as it's likely there will be a very low appetite for risk, however, I would suggest the following:

1. Convince the organisation of the financial value anyway, as they will be accountable for how they spend budgets and likely to be come under a lot of scrutiny anyway. Here are some suggested approaches:
   a. Cyber risk assessment targets investment so that there is no overspend (i.e. no waste of public money) which is common in compliance-based approaches
   b. Cyber risk demonstrates leading thinking in cybersecurity and it is what many of the leading commercial organisations are following today
   c. Reduces the reputational damage from a breach. If you have started to identify the key risk trends to the organisation e.g. *Phishing attacks from outside, Loss of sensitive data from insiders,* then you can start to plan your response to such attacks and ultimately minimize impact. Scenario planning should always be driven by the prioritized risks which are identified from conducting cyber risk assessments.

I don't know how the mechanics of your government work, but there are regulatory bodies that are stipulating the need for cyber risk-based approaches, such as the NYDFS.
https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

If you want to discuss this further just let me know and I'd be happy to discuss.

Continued…

12. How would you coordinate cyber risk prioritisation with enterprise risks?

An approach should focus on the extent to which a cyber risk(s) can affect an enterprise risk(s). There is no universally accepted way of approaching this. There are lots of academic papers that show how to approach such a challenge, but I haven't seen any models that I consider practical – my view only.

What I have seen work well for clients is that they have made a subjective link to the enterprise risks - and it's these enterprise risks that have often influenced the prioritization of the cyber risks. So, they ended up with a 'calculated' cyber risk priority and a 'moderated' cyber risk priority, the latter based on the strength of correlation between a cyber risk and enterprise risk.

To reduce the gap between the cyber risk description and the enterprise risk description, my suggestion would be to categorise the cyber risks under a high-level description. What you want to avoid is explaining how an *SQL injection* impacts *Reputation damage to the enterprise*.

Another feature is that the Moderated risk should be based on the highest individual operation risk rating. See a basic model I've put together to try and explain this further.

Cyber risk category	Calculated Prioritization	Operation risk that can be affected	Extent of influence of the cyber risk	Moderated prioritization of cyber risk
Theft of sensitive data	High	Compliance risk (High) Reputation risk (High) Operational risk (Medium) Legal risk (Medium)	High	High
Loss of availability of key systems	Medium	Compliance risk (Medium) Reputation risk (Low) Operational risk (High) Legal risk (Medium)	High	High
Unauthorised changes to systems access	High	Compliance risk (Medium) Reputation risk (Low) Operational risk (Low) Legal risk (Low)	Medium	Medium

13. There seem to be various components that need to be reviewed and analysed in order to paint a cybersecurity posture to the senior management/board. Do you have a high-level step-by-step guide that allows people to follow the various processes?.. almost like a domino effect way of achieving each step so that things are reviewed/analysed in order?

There are a lot of components to achieving this but here are my suggestions:

1. Conduct an enterprise security review using an industry standard and **make sure** that the approach can be used to benchmark against peers in your industry sector

2. Analyse the data and determine where the control gaps exist (Access control, Supplier assessments, Anti-malware etc)
3. At a high level, determine the risks to your organisation. Again, if you do not have any existing risk assessment processes then I would suggest defining a risk list (say 10 risks such as Theft of sensitive data from insiders, Phishing attacks, Data breach of suppliers etc)
4. Use the risk data to prioritise the control gaps. If there is a control gap that is not going to be exploited by a risk, you have identified then this would be lower priority. Control gaps (e.g. access control) that can be exploited by a risk (e.g. Theft of sensitive data from insiders) would become high priority.

This is a high-level approach, but it provides a logical process to help the business understand which control gaps need to be addressed as a priority – based on the level of exposure to a risk(s). There is nothing that the business won't understand in this approach. It is what business will typically think of when assessing business risk, it's just that other risk disciplines typically do not have the rigour and process to their assessments that we have in cyber risk.

If you wish to discuss in more detail let me know.

14. How do we quantify risk with a "damage to brand" type metric? What have your past clients done?

Quantifying risk for cyber security (as for any risk discipline) requires a solid set of accurate data. In certain areas of risk, such as market risk and insurance risk, this is relatively easy to acquire – which is why many quant models can generate precise information with a high level of confidence.

Without such data a quantitative approach can generate **very precise data** but **very inaccurate answers**, and this is important to note for cyber risk as despite the number of Monte Carlo iterations there are always limits to the amount of accurate data that is available.

However, to quantify the risk associated with damage to a brand, I would suggest unpacking the "damage to brand", so there are factors that should be considered and included in a quantitative model as per below. I also think it is worth considering how damage to brand can extend out to other areas of the business that could be impacted:

- Damage to reputation; extent of negative media coverage, extent of resource reassignment to repair brand (marketing, business development, senior management discussions with tier 1 clients etc)
    - Cost range associated with above £xxxxx - £xxxxxx
- Loss of management control; Impaired decision-making, inability to monitor financial positions, process management failure
    - Cost range associated with above £xxx - £xxxxx
- Loss of confidence by key institutions; Adverse criticism by investors, regulators, customers, or suppliers.
    - Cost range associated with above £xx - £xxx.

These are the types of factors to plug into a quantitative approach. Clients we have worked with before have used similar approaches, especially for their dot com environment where it is easy to determine a range based on past transactions (e.g. loss of a system's availability ranging from 'System is down' for 4 hours during **off-peak trading** through to the same period during **peak trading**).

Some of our clients in the finance and Insurance sectors they have used the approach outlined above.

Contact us: For additional questions or more information about CRMG, please contact us at info@crmg-consult.com or visit www.crmg-consult.com.