Marsh | AFB

Cyber risk governance

How are the UK subsidiaries and branches of non-UK headquartered banks meeting their regulatory obligations?

July 2021

Dr Catherine Raines
CEO, Association of Foreign Banks

Over the past decade, cyber security has emerged as a key issue for businesses in all countries and across all sectors. The financial sector, in particular, is an attractive target for cyber criminals, due to its high dependence on information technology and the potential for substantial monetary gain. As a result, financial sector companies are investing increasing amounts of time and money in strengthening their security and resilience to the threat of cyber-crime. UK regulators have been at the forefront of developing global standards for financial sector cyber security regulation and for the closely related issue of operational resilience. Their outcomes-based approach places an emphasis on governance and the role of boards and management committees in overseeing the response to cyber risk within their companies.

This report examines what this means for foreign banks in the UK operating via subsidiaries or branches, or both. UK boards and management committees are accountable for ensuring that UK regulatory requirements are met, but at the same time much of the technical infrastructure on which they depend — and many of the operational cybersecurity risk controls that protect them — are carried out overseas at group level. In a series of interviews, a representative group of members was asked about the implications of ensuring they meet the standards set out by the UK regulators, in terms of the practical steps that subsidiaries and branches will need to take.

The report identifies several areas of good practice that can help guide individual banks to improve their cyber risk governance approach. Despite the wide diversity in size, business models, and governance structures that characterises the AFB membership, there are common themes that apply to all member banks. This report, commissioned by the AFB and delivered in partnership with Marsh, captures these themes in a maturity model that can be used by individual banks to assess their own cyber governance practices and identify areas for improvement.

The cyber security threat is constantly evolving. The AFB hopes that this report will represent the start of an ongoing conversation between members to share best practice in cyber risk governance and to identify ways in which they can play a part in improving the security and resilience of the UK financial services sector as a whole.

I would like to thank those member banks that contributed to this report, the team at Marsh which prepared it, and in particular Charlie Netherton, Head of Marsh Advisory and Digital, UK and Ireland, for his support.
The AFB will continue to assist our members as they consider this very important topic – and I look forward to ongoing discussions with member banks over the coming months.

Charlie Netherton
Head of Marsh Advisory and Digital, UK and Ireland

The governance of cyber risk is not an easy task for the local boards and management committees of foreign banks operating in the UK. Alongside the inherent challenge of understating a rapidly changing digital landscape is the more specific challenge of establishing clearly what falls within the remit of the local leadership team and what sits at group level.

While many banks are centralising more and more of their IT functions to the group or to wholly owned operational subsidiaries operating at group level, UK leadership must remain responsible for ensuring that the potential risks to the bank's UK operations are properly understood and managed. Not only is this a clear requirement of UK financial sector regulation, it also reflects the fact that UK leadership are in the best position to understand local circumstances and how UK stakeholders could be impacted by a significant cyber event. Indeed, as is argued in this report, the greater the level of centralisation of IT, the greater the emphasis that needs to be placed on local risk management oversight.

The overarching danger for UK subsidiaries and branches of foreign banks is that assumptions could be made about how responsibility and accountability is distributed between group and subsidiary/branch level. Senior managers at group and local level need to "mind the gap" and ensure that there is proper dialogue on this issue between the UK branches and their parent overseas.

In this survey of foreign banks operating in the UK, we have found a range of different approaches that boards and management committees have taken to addressing this issue. While there are many factors that will determine the best approach for any individual entity, there are some fundamental processes that we believe all foreign banks need to address if they are to have confidence that the cyber risks associated with their UK operations are being managed effectively — namely:

- Understanding how differences in local-level and group-level cyber risk exposure are identified and addressed.
- Defining how intragroup responsibilities and accountabilities are defined and managed.
- Ensuring that the UK board or management committee has the right level of oversight of relevant control activities (at both local and group level).
- Ensuring that the UK board or management committee is adequately prepared to deal with major cyber events when they occur.

We hope that this report provides a catalyst for further discussion among the foreign banking community in the UK about best practice cyber risk governance and how subsidiaries and branches can work together to enhance the security and resilience of the UK financial sector as a whole.

I would like to thank the AFB and their members for their contribution and sponsorship, and Jamie Saunders and the rest of the Marsh team for their hard work in producing this insightful report.

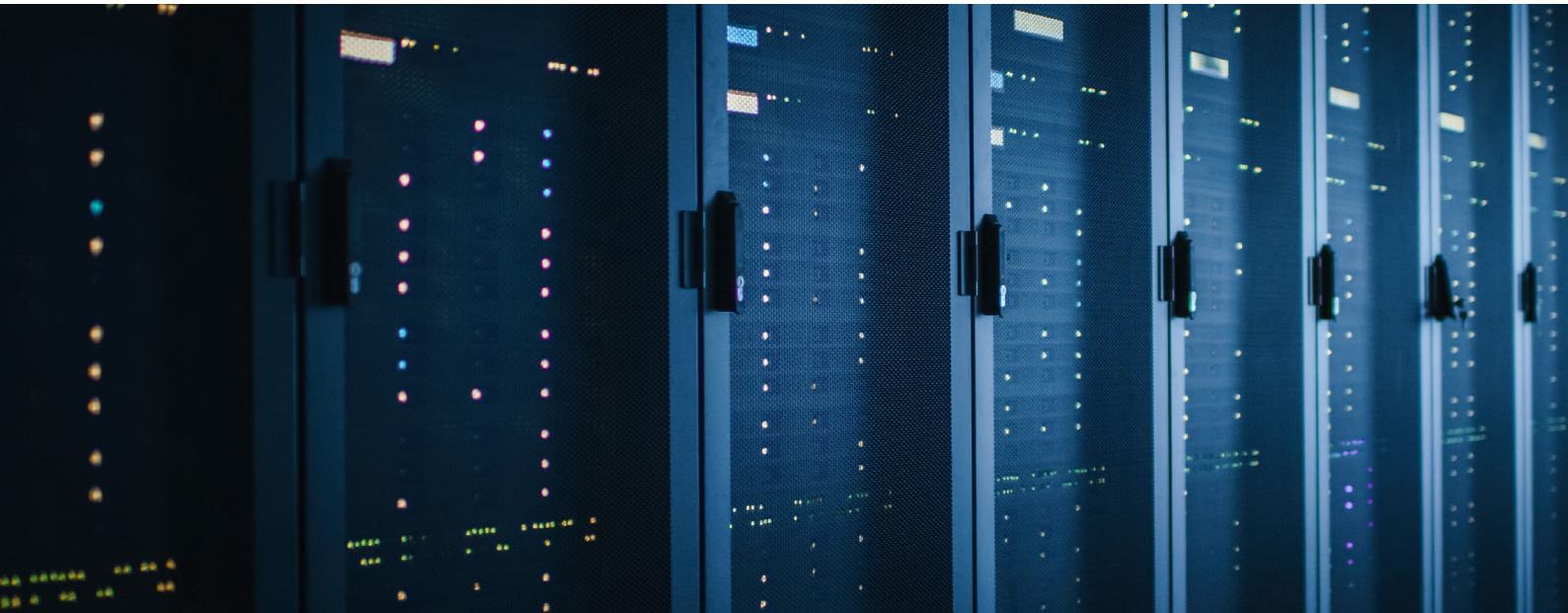
Contents

Introduction

This report brings together findings from a series of interviews conducted in March and April 2021 with members of the Association of Foreign Banks exploring how UK subsidiaries and branches of non-UK headquartered banks can meet their regulatory obligations relating to cybersecurity. This task can be particularly challenging for subsidiaries and branches when much of the technical infrastructure and many of the operational cybersecurity risk controls are carried out overseas at group level.

Throughout the interviews, we took a broad interpretation of the term "cybersecurity" and "cyber risk". While the term "cyber" is often associated with deliberate attacks by nefarious actors, what usually matters most to banks is the impact on their operations, which does not necessarily depend on whether a cyber event was deliberate or accidental, or whether it was caused by an external actor or by mistakes made within the bank. In its most general sense, "cyber risk" refers to risks arising from a bank's dependency on data and IT, and cybersecurity refers to the steps that are taken to mitigate these risks.

The need for cybersecurity has risen dramatically in prominence over the past 10 years, and consistently appears at or near the top of business surveys of corporate risk. The issue is demanding more time of company executives and boards of directors and is subject to greater regulatory attention. And rightly so: as our economies and societies grow more and more dependent on digital technology, it is important to ensure that the risks associated with this are properly managed and mainstreamed into corporate governance.



The Bank of England, PRA, and FCA have been at the forefront of developing global standards for financial sector cyber regulation. Their outcomes-based approach places an emphasis on governance issues and the role of boards and management committees in overseeing the response to cyber risk within their companies.

For several years, governments and industry bodies have provided standards and best practice guidance for specialists in the IT and security departments, but these do not necessarily provide much support for boards and management committees who will not be intimately involved in day-to-day IT and security operations (and may not have much experience working in these disciplines during their careers). It can often be a challenge to translate the language of cybersecurity (ones and zeros) into the language of business (pounds and pence). More recently, there has been guidance aimed specifically at boards to help them in their role, including The World Economic Forum's 2017 report "Advancing Cyber Resilience: Principles and Tools for Company Boards"; the Marsh and TheCityUK 2018 report "Governing Cyber Risk a guide for company boards"; and the UK National Cyber Security Centre's "NCSC Board Toolkit".

While all of this guidance is helpful, it is not always clear how boards and management committees of foreign banks operating in the UK can provide effective oversight and assurance when much of the technical infrastructure and many of the security risk controls are managed outside of their purview. As far as the regulators are concerned, the requirements are clear: boards and management committees cannot outsource their responsibilities for managing risk and, in this regard, group-level services need to be treated just like any other third-party service provision. How can subsidiaries and branches square this circle?

The overarching danger is that assumptions could be made about how responsibility and accountability are distributed between group level and subsidiary/branch level. Senior managers at group and local level need to "mind the gap" and ensure that there is proper dialogue on this issue between the UK and their parent overseas.

Once accountabilities have been clarified, the question becomes how UK boards and management committees fulfil these obligations in practice. In this report, we set out the various different governance structures that currently exist within a sample of the foreign bank community in the UK, and we examine the different ways in which the banks interviewed have responded to this challenge.

In our analysis, we categorise these responses into four sets of activity — or dimensions — that can help UK banks to determine how effectively they are meeting their cyber risk governance responsibilities. These are:

Risk management: how differences in local-level and group-level cyber risk exposure are identified and addressed.

Governance of intragroup relationships: how intragroup responsibilities and accountabilities are defined and managed.

Assurance: what oversight the UK board or management committee has of relevant control activities (at both local and group level).

Preparedness: how well prepared the UK board or management committee is to deal with major cyber events when they occur.

For each of these dimensions, we assess the practices of the UK banks interviewed against a set of maturity levels – the higher the level, the better the bank is able to demonstrate good governance of cyber risk. The percentage of banks at each level is captured in a series of charts that boards and management committees can use to assess where they stand relative to their peers.

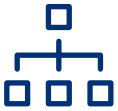
We close the report with some recommendations for next steps by AFB member banks.

Context – the role of subsidiary boards and branch management committees

Subsidiary boards and branch management committees carry ultimate accountability for ensuring that UK regulatory requirements are met. The practical means by which this can be achieved, however, are highly dependent on the way in which the subsidiary or branch operates within the group as a whole.

Ensuring clarity around these contextual issues is an important first step in ensuring that the governance of cyber risk properly reflects the subsidiary's or branch's circumstances.

In our interviews we identified various factors that influence the approach that the UK branch or subsidiary takes to governing its cyber risks:



Regulatory requirements and standards in the UK

- Is the entity a branch or a subsidiary (or, in the case where multiple entities sit under a single UK board or management committee, a combination of both)?
- Is the entity solo- or dual-regulated within the UK?
- How comparable are the regulatory requirements in the UK to those pertaining in the group's HQ jurisdiction?

Relationship between the UK entity and the group

- What is the nature of the UK entity's operations in the UK? Is this broadly comparable to the group's operations in its home market, or is it limited to a subset of activities (for example, the UK bank may focus solely on wholesale operations while the parent is conducts both wholesale and retail operations)?
- How critical is the UK entity to the profitability of the group as a whole, or to the viability of key lines of business?
- How do the responsibilities of local management relate to functional management at group level? How is this reflected in funding and budgetary authority?
- What level of influence does the UK board or management committee have over decisions made at group level (formally or informally)?

IT management

- What is the balance between centralised and localised IT?
- Are there systems or applications that are unique to the UK?
- Does the UK entity have responsibility for any group-wide applications? To what extent is local management accountable for overseeing these?

Risk management

- Does the UK subsidiary or branch have an independent risk management function?
- Do all 3 Lines of Defence operate in the UK?
- To what extent are they involved in the management of cyber risk?

While these contextual factors vary considerably from bank to bank, depending on their size and the nature of their UK operations, the fundamental requirement for UK banks to ensure that the risks associated with their operations are properly managed remains constant.

Four dimensions of cyber risk governance

In our interviews we identified several measures that UK entities are taking to improve their governance of cyber risks. We have categorised these into four sets of a dimensions that describe different aspects of cyber risk governance.

For each dimension we define maturity levels, which can be used to assess their cyber governance performance and compare this to their peers. These maturity levels can be applied irrespective of how the subsidiary or branch operates in the UK, but of course the individual choices that they make about how they implement them will depend on their circumstances and the nature of their relationship with their parent – some of the different options we identified during the interviews are given below. Alongside the maturity levels and implementation options we provide a set of questions that boards and management committees can ask themselves in order to assess their own maturity level.

The four dimensions are:

Risk management

How differences in local-level and group-level cyber risk exposure are identified and addressed.

Governance of intragroup relationships

How intragroup responsibilities and accountabilities are defined and managed.

Assurance

What oversight the UK board or management committee has of relevant control activities (at both local and group level).

Preparedness

How well prepared the UK board or management committee is to deal with major cyber events when they occur.

Common themes across all of these dimensions are:

- The need for a localised view of risks, control effectiveness, and preparedness.
- The need for clarity regarding the responsibilities of the local management team versus the responsibilities that are held at group level.
- The need for the local team to have the skills, support, and management information needed to equip them to fulfil their roles.

DIMENSION 1

Risk identification and establishment of cyber risk controls

Under UK financial sector regulation, subsidiaries, and branches are responsible for ensuring that "all risks to cyber security are translated into and managed within the enterprise risk framework". They are also responsible for ensuring that "these are aligned to enterprise-level risk appetite statements and reassessed on an ongoing basis" [CQUEST questionnaire 2019].

Risk identification

It cannot be assumed that cyber risks at the subsidiary or branch level are identical to those at group level. In practice, it may be that local cyber risks are simply a subset of group level cyber risks, but even then, local circumstances may dictate a different risk appetite. As well as the possibility of material differences in operational risk exposure, UK regulation can sometimes be more demanding than the regulations pertaining to a bank's headquarters jurisdiction. For these reasons it is necessary for the UK board or management committee to have its own view of cyber risk. It is worth noting that the UK often acts as a standards-setter when it comes to financial sector regulation, and so requirements that originate in the UK are often later adopted elsewhere. While the need to meet more stringent regulations in the UK may be perceived as an unwelcome cost of doing business, it can help prepare organisations for requirements that will become more widespread over time.

There are several practical ways in which boards and management committees can develop their own localised perspective on cyber risk:

- Some banks have developed sets of risk libraries at group level. Individual subsidiaries and branches then draw down the risks that are relevant to their local operations, adapting risk appetite as required to reflect local circumstances.
- Some subsidiaries and branches take more of a localised approach, where risks are identified independently from group level risk identification activity. This may be appropriate where there is a high degree of operational independence between local and group level, where regulatory requirements are significantly more demanding in the UK than in the HQ jurisdiction, or where there is a lack of mutual recognition of regulatory practices between jurisdictions.
- A hybrid approach whereby risks are identified at local level, and then mapped onto the group level risk register. Any gaps are either recorded locally or delegated upwards to be incorporated into the group level risk register.

When identifying cyber risk at the local level, it is important to consider not only how incidents at group level could affect the subsidiary or branch, but also how incidents at the subsidiary or branch level could affect the group as a whole, especially if there are activities at local level that carry more inherent risk.

It is also important to ensure that front line business units are involved in the risk identification process – they are usually in a better place than the IT or security departments to assess the potential impact of an adverse cyber on their operations, and so can help to ensure that the right risks are prioritised.

Risks should be quantified where possible. The potential impact of a worst-case scenario on subsidiary or branch finances should be understood. It should be clear how the costs of such scenarios would be paid for and (for subsidiaries) how this is reflected in capital requirements.

Establishment of cyber risk controls

The UK board or management committee is responsible for ensuring that a control framework is in place that addresses the principal cyber risks that have been identified.

It is likely that the majority of technical cyber risk controls will be conducted alongside management of the IT systems to which they relate – in other words, a centralised approach to the provision of IT will generally lead to a centralisation of technical control activities.

This is not necessarily the case when it comes to procedural controls, such as processes for granting privileged access to systems and processes for on-boarding and off-boarding staff. Likewise, physical access controls are more likely to be conducted locally than at group level. Compliance monitoring may be conducted locally or centrally – although clearly local management have an important role in enforcing compliance via local line management oversight.

The UK board or management committee needs to ensure that there is clarity around what controls are operated locally and what are operated centrally.

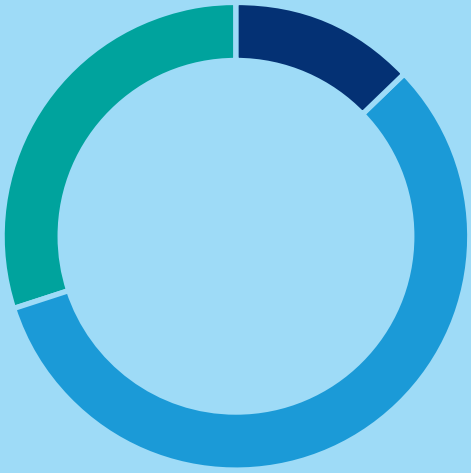
Irrespective of where controls are implemented, the board or management committee is responsible for ensuring that "effectiveness of cyber security controls has been independently assessed by a party with the competent level of skill and forms part of an established annual process, including senior executive review" [CQUEST questionnaire 2019].

For this reason, as more and more technology and first line risk controls are centralised, more focus needs to be placed at subsidiary and branch level on second and third line risk management and assurance.

In practice (and especially for smaller subsidiaries and branches), much of the work to develop controls and assess control effectiveness will be conducted in the group's headquarters jurisdiction. The question therefore arises as to whether the UK board or management committee can depend on group level assessments to judge the adequacy of the group's controls framework against UK regulatory requirements. Several of the banks interviewed had chosen, as a matter of policy, to set requirements across the group according to the most stringent regulations within any of the jurisdictions where they operate. Where there is a high degree of compatibility and cooperation between regulators, this enables UK boards and management committees to draw on supervisory activities within the headquarters jurisdiction to help demonstrate that UK requirements are being met. Where there is a high level of divergence between regulatory requirements in the group headquarters jurisdiction and the UK then it is more likely that the UK subsidiary or branch will need to take additional steps to ensure that UK requirements are met – either by shaping what is done at group level, or by implementing supplementary controls at local level.

01| Risk identification and establishment of cyber risk controls

The following chart summarises the different levels of maturity and some of the different implementation options that we observed during the interviews with AFB members, as well as the key questions that the board or management committee should examine when considering how cyber has been integrated into enterprise risk management.



Source: *Marsh*

Implementation options

1. Bespoke cyber risk register and control framework developed by the UK bank.
2. Use of group level risk libraries, adapted as necessary to fit local risk tolerances and regulatory requirements.
3. Hybrid approach, combing a mix of locally developed and group-level risk registers and risk controls.

Key questions for the board or management committee

- Do you understand the group's priorities and strategic approach to cyber risk?
- Do you have a clear understanding of how UK operations could be impacted by cyber events (occurring either locally or at group level)?
- Do you understand what controls are in place at group level to manage cyber risks, and have you determined if any additional controls are required at local level to complement group level activity?
- Do you understand the regulatory requirements in the UK relating to cyber risk management and how these affect your own responsibilities?

MATURITY LEVEL

Level 1 13%

- Cyber risks facing the bank's UK operations have not been assessed.
- The UK banks has limited visibility of the group's cyber risk register.
- The UK bank is dependent on group level controls but has limited direct visibility over them.
- The cyber risk control framework takes no account of specific UK regulatory requirements.

Level 2 57%

- The UK bank has assessed the group cyber risk register to determine whether it addresses UK operational needs and regulatory requirements.
- Where relevant, risks that are unique to the UK bank have been identified.
- The UK bank has visibility of the group-level control framework and has implemented local measures to address gaps.

Level 3 30%

- Cyber risks associated with the bank's UK operations have been explicitly defined and are incorporated into the bank's enterprise risk management framework at local and group level.
- Controls at local and group level have been formally assessed against the UK bank's operational needs and regulatory requirements. Adjustments have been made at both group and local level to address gaps.
- All relevant parts of the UK business have been engaged in the risk identification process and are accountable for implementing local cyber risk controls in their area.

2

DIMENSION

Governance of intragroup relationships

Local leadership accountabilities

Subsidiaries and branches of foreign banks operating in the UK will often be subject to complex lines of accountability. Some individual board or committee members may be subject to specific UK Senior Managers and Certification Regime (SM&CR) requirements. Boards and management committees are accountable for ensuring that the UK operation delivers on the strategic priorities that have been set for it by the group.

The SMF24 Chief Operations Function has overall responsibility for managing the internal operations or technology of the firm, generally including IT, cybersecurity, and business continuity. The person performing this function should have "sufficient expertise and authority to perform that function effectively" [FCA Handbook SUP.10C.6B]. In practice, branches may have more flexibility than subsidiaries to determine how SMF accountabilities are assigned – in particular, it is legitimate for responsibilities to be held by a person outside of the UK, although that person would be expected "to spend an adequate and proportionate amount of time in the UK to ensure that relevant activities are suitably controlled" [FCA paper "Our Approach to International Firms, February 2021].

The UK subsidiary or branch is usually also responsible to the group for ensuring that any cybersecurity controls that are delegated to the subsidiary or branch are operated effectively, and that compliance with group-wide cybersecurity policies is upheld.

The UK subsidiary or branch may be responsible for operating specific functions or systems on the whole of the group's behalf. This could include systems that support activities that are wholly or largely conducted in the UK (for example, certain categories of trading), but it could equally include activities that are conducted across the group. In such cases, local management need to understand what they are and are not responsible for in terms of operating systems and in terms, of ensuring that risks to the whole group are being managed effectively.

Finally, the UK's role as a global financial centre means that many of the specialist skills required to run a successful bank are well represented in the local employment market. Several firms have hired UK based staff to undertake group-wide roles, including for IT and security. Several larger groups operate on a divisional basis, which cut across geographical boundaries. COVID-19 pandemic travel disruptions have also blurred the boundaries between places of work. The question therefore arises as to the extent to which UK based management are accountable for activities that take place in the UK but for which they are not directly responsible, including in particular the extent to which they are accountable for ensuring that these activities are conducted in accordance with group-wide policies (including cybersecurity policies).

What is clear is that, irrespective of how the UK subsidiary or branch is governed, and irrespective of its relationship to the group, local top leadership carry some responsibility for cybersecurity. It is not a responsibility that can be entirely left to group level. What matters is that "All [such] roles, accountabilities and responsibilities [should be] clearly defined, documented and assigned" and "all senior executives [should be] aware of these and their understanding is validated" [CQUEST questionnaire 2019]. In particular, there needs to be clarity around the division of responsibility between UK subsidiary or branch and headquarters.

Intragroup outsourcing service-level agreements (SLAs)

Increasing emphasis on operational resilience within the UK financial sector (along with increasing concerns across the whole economy around supply chain security and outsourcing) has resulted in a new focus on intragroup outsourcing. This is reflected in the publication in March 2021 of Prudential Regulation Authority (PRA) Supervisory Statement 2/21 on outsourcing and third-party risk management.

PRA SS 2/21 makes it clear that "intragroup outsourcing is subject to the same requirements and expectations as outsourcing to service providers outside a firm's group" and that they "should not be treated as being inherently less risky".

PRA SS 2/21 comes into effect on 31 March 2022. At that time, firms will be expected to have documented all of its material outsourcing arrangements, and for these to be supported by "agreed service levels [such as SLAs], which should include qualitative and quantitative performance criteria and allow for timely monitoring, so that appropriate corrective action can be taken if these service levels are not met". There is also specific mention in SS 2/21 of the need for banks with headquarters in the EU to comply with these requirements as part of their post-Brexit transition to formal 3rd country branch status.

SMF: Senior Management Function

Practical leverage, influence, and relationships

While accountability statements and formalised SLAs can provide UK boards and management committees with a significant leverage, the extent to which local requirements and concerns are taken on board at group level will depend on the nature of the formal and informal relationships between the key players involved.

This in turn will depend to a degree on the role that the UK subsidiary or branch plays in the overall group, in other words, it is context dependent. PRA SS 2/21 cites a number of factors that can determine the practical degree of control and influence, including "the level of connectivity between the UK entity and the group level board, board committees, executive committees, internal control functions and/or other relevant functions (e.g. technology)". Although not stated explicitly in the PRA SS 2/21, it was clear from our interviews with AFB members that personalities and personal relationships can also play an important role in establishing the right level of influence from subsidiary or branch to parent.

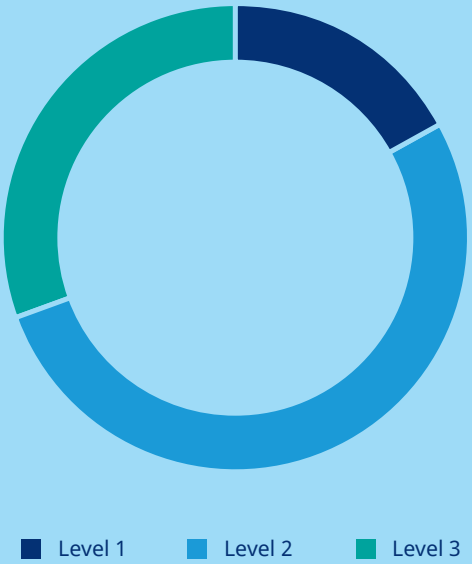
What matters is that:

- The degree of influence that the UK subsidiary or branch has over the group is commensurate with the role that the UK plays in the group's overall strategy.
- The degree of influence is sufficient to enable the board or management committee to satisfy UK regulatory requirements.

If there is any doubt that the degree of influence is sufficient to meet regulatory requirements, or that it is somehow not commensurate with the role that the UK plays in overall group strategy, then this should be escalated to group level.

02| Governance of intragroup relationships

The following chart summarises the different levels of maturity and some of the different implementation options that we observed during the interviews with AFB members as well as the key questions that the board or management committee should examine when considering how cyber is addressed in the governance of intragroup relationships.



Source: *Marsh*

Implementation options

1. Risk management and risk controls fully delegated to the UK bank.
2. 2nd line risk management functions at UK bank level, with 1st line controls outsourced to the group and governed via SLAs.
3. SM&CR roles held at group level.

Key questions for the board or management committee

- Is it clear what responsibilities for cyber risk management are held locally and what are held at group level?
- Are SLAs in place to ensure that relevant risk control activities at group level are sufficient to meet the UK bank's needs?
- Are you able to exert an appropriate level of influence over group level risk control activities?

MATURITY LEVEL

Level 1 17%

- No specific responsibilities for cyber risk governance have been allocated to the UK board or management committee.
- There is no formal record of the group-level services on which the UK bank's operations depend.
- The UK bank has limited influence over the group's overall approach to managing cyber risk.

Level 2 52%

- The UK board or management committee's accountability to UK regulators are understood, but their ability to affect relevant activities at group level may be unclear.
- The group-level services on which the UK bank depends have been catalogued, but formal SLAs have yet to be agreed.
- The UK bank is able to escalate concerns about weaknesses in the group cyber risk control framework and generally receives a good response.

Level 3 31%

- The respective responsibilities for cyber risk governance between group and local level leaders are fully understood and effective mechanisms are in place to ensure accountability.
- Intragroup SLAs have been fully established and communicated.
- The influence that the UK bank has on group level cyber policy and strategy addresses the need to satisfy UK regulatory requirements and reflects the status of the UK bank within the group.

DIMENSION

3

Assurance

Group-wide assurances

Any assurance that is available at group level will provide comfort to a UK board or management committee. Depending on the degree of coordination between regulatory authorities, this can provide evidence that can be used by the UK regulators when undertaking their supervisory role. Indeed, this approach is common practice for regulators who work together to supervise the largest global banks.

Likewise, group-wide penetration test and red teaming exercises can provide good evidence of control effectiveness at the local level.

Such group-wide assurances are only valid to the extent to which the risks and risk appetites at UK level align with the risks at group level. This is why having a localised risk register is so important — this will enable the UK board or management committee to focus its own assurance activities on areas of divergence.

Local penetration testing

Most of the firms interviewed conduct some form of penetration testing programme. Such tests are broadly recognised as providing some of the best independent assurance available, and they have formed part of the PRA's supervisory regime for several years.

It cannot, however, be assumed that centralised penetration testing programmes will address the specific risks or operating circumstances of the UK subsidiary or board. There is therefore merit in boards and management committees sponsoring their own penetration testing exercises in order to ensure that the controls of most relevance to their local cyber risks are properly evaluated. This may be a matter of the UK subsidiary group being able to task a centralised penetration testing programme, or it might be a matter of conducting independent penetration tests locally. If the latter, then it is important to ensure that centrally managed systems on which the UK subsidiary or branch depends are within the scope of the local penetration testing programme.

Management information

Most of the UK boards and management committees interviewed have at least some visibility of the Management Information Reporting provided by group level risk managers to the group board. While useful, such reporting does not really provide UK-based leaders with the information that they need to judge how well UK-specific risks are being managed. Neither do they necessarily provide much insight on UK compliance with group-level cybersecurity policies. In effect, this makes it difficult for them to fulfil their fiduciary and regulatory responsibilities.

Whilst it is hard to define a single best practice template for management information reports, the following highlights some of the information that UK boards and management committees should expect to see on a regular basis:

- A statement of compliance with UK statutory and regulatory requirements.
- A statement of compliance with relevant group level policies and standards (including how UK compliance compares with other parts of the group).
- A localised risk report showing any divergence with subsidiary/branch risk tolerances, alongside progress against any planned mitigation measures.
- Indicative technical performance measures, such as breaches, service outages, and near misses, as they relate to UK operations.
- The outcomes from penetration testing and incident management exercises (be they local or group level).
- Relevant third party supply chain risk assessments, including performance against SLAs - including intragroup SLAs.
- Strategic threat intelligence, including emerging threats that are relevant to the bank's UK operations, and insights from significant cyber events impacting on peers in the sector.

Local expertise within the 3 Lines of Defence model

Subsidiaries and branches vary to the extent that there is local expertise on IT risk within the first, second, and third lines of defence. As IT functions have become increasingly centralised, it becomes more important to ensure that there is sufficient expertise in the second line to hold group level first line teams to account. While the UK regulators recognise that specialist third line IT auditors may, by necessity, be centralised at group level, it should nonetheless be possible for the UK board or management committee to task them directly to investigate matters of particular concern at local level.

MATURITY LEVEL

Level 1 — 26%

- Cybersecurity assessments are conducted at group level, but these do not take account of specific UK requirements.
- The UK bank has no independent penetration testing activity and little influence over what is tested in the group level programme.
- The UK bank has limited visibility of group level Management Information and what it sees does not illuminate relate to UK cyber risks or control performance.
- There is limited expertise on cyber risk in the UK bank.

Level 2 — 61%

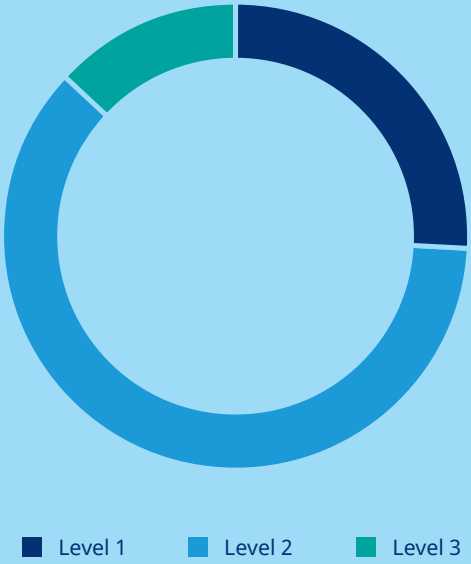
- Cybersecurity assessments at group level take account of UK specific requirements. UK-based cybersecurity assessments may also take place.
- The UK bank is able to place requirements on the group level penetration testing programme and may also have its own local programme.
- Management Information is available to the UK bank, but may not be sufficiently granular to illuminate local-level issues.
- There is local expertise on cyber risk within the UK bank, but there may be limited access to skills in one or more of the three Lines of Defence.

Level 3 — 13%

- Systems of most relevance to the UK bank's cyber risk exposure are regularly tested (this may be part of a group-level of local programme).
- Management Information is generated at both local and group level. Group level MI is sufficiently granular to illuminate issues specific to the UK bank.
- The UK bank has direct access to cyber expertise in all three lines of defence (may be at local or group level).

03| Assurance

The following chart summarises the different levels of maturity and some of the different implementation options that we observed during the interviews with AFB members, as well as the key questions that the board or management committee should examine when considering its need for cyber assurance.



Source: *Marsh*

Implementation options

1. The UK Bank is dependent on security attestations from the group.
2. The UK bank conducts a range of local assurance activities to complement activities at group level.

Key questions for the board or management committee

- Do you have access to the skills you need to identify local risks and assess local and group level control effectiveness?
- Do you receive Management Information that effectively illuminates cyber risk at the UK bank level?
- Have your most critical systems been penetration tested?

Preparedness

4 DIMENSION

Operational Resilience

On 29 March 2021, the PRA and the FCA published policy documents on operational resilience, following an extended consultation period. A shared policy summary paper was published on the same date entitled "PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services". The UK policy approach is consistent with the Basel Committee on Bank Supervision's report "BCBS Principles for resilience" published on 31 March 2021.

The regulators' approach to operational resilience is centred on the need for preparedness. It is "based on the assumption that disruptions will occur, which will prevent firms and FMIs [(Financial Market Infrastructures)] from operating as usual, and result in them being unable to provide their services for a period. The supervisory authorities consider that many firms and FMIs currently may not sufficiently plan on the basis that disruptions will occur, and therefore would not be able to manage effectively when they do."

The framework set out in the original consultation documents requires firms to:

"Identify their important business services by considering how disruption to the business services they provide can have impacts beyond their own commercial interests; set a tolerance for disruption for each important business service; and ensure they can continue to deliver their important business services and are able to remain within their impact tolerances during severe (or in the case of FMIs, extreme) but plausible scenarios."

As the UK is ahead of many other jurisdictions in terms of setting operational resilience requirements, UK boards and management committees cannot assume that these requirements are being or will be met at group level. Some banks that we interviewed said that they were adopting the UK approach to operational resilience at a group-wide level, in anticipation that these requirements will become more widespread over time. Even where there is work on this issue at group level, UK boards and management committees need to ensure that business services that are deemed important for the bank's UK operations, or that have the potential to cause intolerable harm to clients in the UK or to the UK financial system if they go wrong, are attracting the right level of attention at group level.

It is therefore necessary for UK boards and management committees to conduct their own assessment of what is and is not within scope of these new requirements. It is important to ensure that third party services (including intragroup services) are included in these assessments.

Crisis management and crisis exercises

Most of the banks interviewed have crisis management processes in place for their UK operations, often based on concerns for business continuity in the event of physical disruptions to their offices or staff. Many banks mentioned that the COVID-19 pandemic had stress-tested these processes, and that generally their banks had responded well.

A major cyber related crisis will inevitably require action from the UK management committee and, in the case of subsidiaries, may well require action from the board. It is important to ensure that:

- There is a common understanding of when and how individual cyber incidents should be escalated and when corporate crisis management processes invoked.
- There is clarity of decision making responsibility and authority between group and UK legal entity boards.
- Top leadership has the information that it needs to respond effectively (including, for example, easily accessible information about the nature of the data held by the bank and the location of key systems, and the role played by critical third party suppliers).
- There is ready access to external expertise (technical but also, for example, legal and strategic communication advice).

A good way of evaluating leadership crisis preparedness is to conduct crisis management exercises. Most of the banks interviewed do conduct crisis management exercises, and many have conducted crisis exercises based on cybersecurity scenarios. However, many of the exercises did not include board or management committee participation, leaving questions about what their role should be in the event of a major cyber incident.

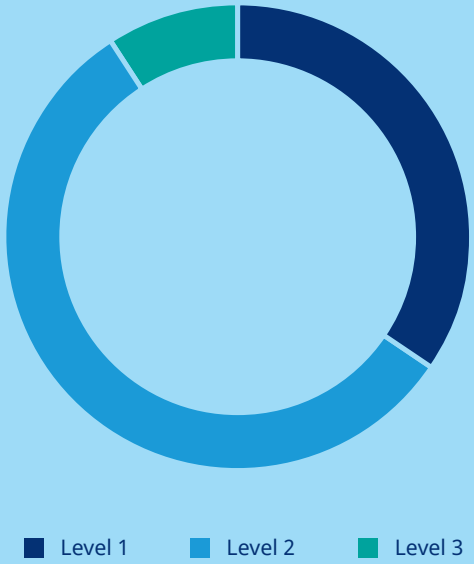
Crisis financing

Major cyber events can incur significant direct and indirect costs. Quantifying cyber risk exposures can help firms to undertake crisis planning and prioritise mitigating actions.

Subsidiaries will generally need to reflect the potential costs of worst-case cyber scenarios within their capital allowance calculations. For branches, it is important to establish how crisis response will be financed — at branch or at group level. In both cases, it is worth establishing what protection is provided by the company's insurance programme.

04| Crisis preparedness

The following chart summarises the different levels of maturity and some of the implementation options that we observed during the interviews with AFB members, as well as the key questions that the board or management committee should examine when considering its preparedness for a major cyber event.



Source: *Marsh*

Implementation options

1. Operational resilience of the group is defined by the toughest regulations.
2. Operational resilience of the entire group is defined by the group's jurisdiction's regulatory requirements.
3. Operational resilience differs at group and branch / subsidiary level based on the entity's own jurisdiction.

Key questions for the board or management committee

- Do you understand what role you would be expected to play in a major cyber crisis impacting on the UK bank's operations?
- Have you had an opportunity to exercise your personal preparedness for such an event?
- Have you satisfied the requirements of PS6/21 | CP29/19 | DP1/18?
- Have you assessed the potential cost of a major cyber event affecting UK bank operations and how this would be paid for?

MATURITY LEVEL

Level 1 35%

- The process to identify the UK bank's Important Business Services has not yet started.
- While local crisis management processes may exist, these have not been tested against a range of plausible cyber related crisis scenarios.
- The UK board or management committee have not been involved in crisis exercises with a cyber component.
- The cost of a plausible worst case cyber scenario has not been assessed.

Level 2 56%

- Important Business Services are in the process of being identified and impact tolerances set.
- Crisis management processes exist and have been assessed against a range of plausible cyber scenarios.
- The cost of a plausible worst case cyber event on the UK bank has been assessed and relevant provisions to cover the cost have been made at either group or local level (this may include an insurance component).

Level 3 9%

- Important Business Services are on track to be identified and impact tolerances set by the March 2022 deadline. Where these services are dependent on intragroup outsourcing, SLAs have been agreed.
- Cyber crisis exercising has taken place and has included relevant actors at group level. The branch / subsidiary may have its own cyber insurance policy, defined by clear cyber exposure quantification.
- The UK board or management committee have been involved in crisis exercising.

Analysis of the results from the interviews

All of the companies we interviewed are making good progress with cyber risk management and have recognised the need to establish the right level of in-country expertise to ensure that that UK-specific risks are identified and addressed within the group-level and local-level control framework.

Recent interventions by the UK regulators have helped to drive this progress, including the focus on Operational Resilience and outsourcing. The need for EU based banks to transition to third country branch status has also played a role.

There are, however, material differences in the extent to which UK subsidiaries and branches have embedded cyber risk within their formal governance arrangements. These differences include the extent to which local risk registers have been developed, the extent to which local requirements are reflected in the group level risk control framework, whether there are formal SLAs in place to cover critical intragroup outsourcing arrangements, and whether the management information reporting received by UK boards and management committees takes sufficient account of local needs.

We have assessed each of the UK banks that we interviewed and have assigned them a score against the maturity levels outlined above. These results show that most banks have mapped their local cyber risk exposures, and that some good progress has been made on assigning and documenting responsibilities at local and group level. Of more concern are gaps in assurance, for instance it may be clear what the UK entity's risks are and how these need to be controlled, but it is more difficult to establish whether these controls are being effective in meeting the UK entity's specific requirements.

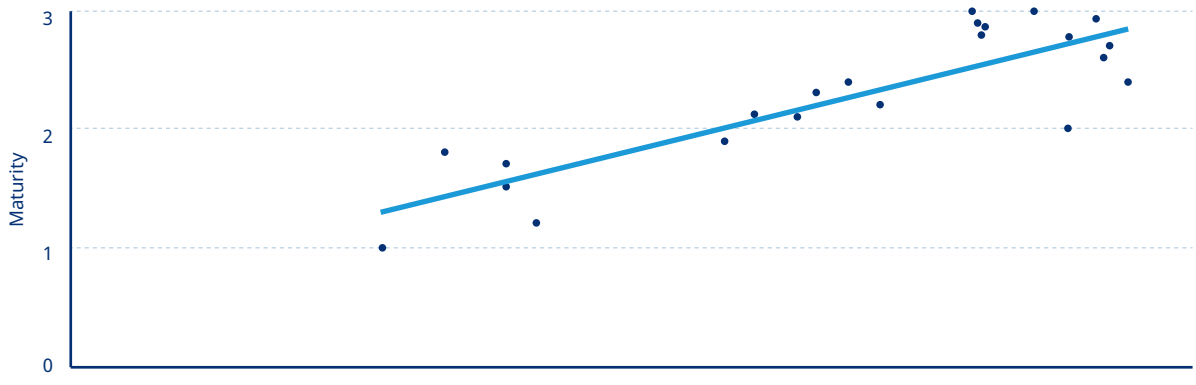
Several of the AFB members that we interviewed observed that more of their operational IT was being centralised at group level, meaning that local management had less visibility of how these systems and associated risk controls were being managed. Some recognised that this had the potential to exacerbate gaps in their local assurance coverage and had responded to this by strengthening their specialist second line of defence teams in the UK.

We also observed a gap in preparedness: Several banks mentioned that they had been intending to improve their cyber crisis management planning, but that the need to respond to the pandemic had got in the way. Many also remarked that the pandemic had enabled them to live-test their operational contingency measures. Notwithstanding this, we noted from the interviews that UK firms should still be putting greater focus on crisis planning, given that there is a wide variety of cyber-related scenarios that could impact on the bank, and that it cannot be assumed that the pandemic response will have covered all of these.

Finally, we explored the relationship between the different banks' circumstances and the overall maturity of their approach to cyber risk governance. Two themes emerged from this analysis:

- Banks that are headquartered in jurisdictions with the most developed financial regulatory systems tend to take a more centralised approach to risk management. In most of these cases, the group have chosen to adopt a superset of the most stringent regulations from the jurisdictions in which they operate and to apply these across the whole of their operation. The significance for UK subsidiaries and branches is that the most stringent requirements often originate in the UK, giving the UK board or management committee the opportunity to have additional influence over group level standards and policies.
- Perhaps unsurprisingly, there was a correlation between the maturity of a UK bank's approach to cyber governance and the importance of the UK market to the group's strategy and profitability. One reason cited for this was the overarching priority given by the group to UK boards and management committees to maintain robust compliance with UK regulatory requirements, and the high levels of support are provided from the group to ensure that this objective was achieved. UK banks in this category tended to have the highest level of investment in second (and, in some cases, third line) resources at the UK subsidiary or branch level. This correlation is illustrated in the following chart:

05| Correlation between cyber governance maturity and the strategic importance of the UK bank to the group



Source: *Marsh*

Conclusions and recommendations

The responsibility on UK boards and management committees is clear: they carry ultimate accountability for ensuring that UK regulatory requirements are met.

The danger is that assumptions could be made about how responsibility and accountability is distributed between group and local level. Top leaders at both ends of the relationship need to "mind the gap" and ensure that there is proper dialogue on this issue between group and local level.

There is a set of key questions, derived from the interviews we conducted during this survey, which will help individual AFB members to benchmark where they stand against their fellow foreign banks. These are given in the tables above; board and management committees may wish to spend some time going through these questions in detail with relevant experts within the UK bank and at group level.

To provide a quick self-assessment, readers may find it useful to consider the summary questions below:

- Do you have a clear understanding of how UK operations could be impacted by cyber events?
- Do you understand the group's priorities and strategic approach to cyber risk?
- Can you describe your personal responsibilities for managing cyber risk?
- Do you have the information you need to determine whether the control activities taking place locally and at branch level are sufficient to meet the UK bank's needs?
- Are you able to exert sufficient influence over the group to ensure that any control or assurance gaps are addressed?
- Do you understand what role you would be expected to play in a major cyber crisis impacting on the UK bank's operations, and how well prepared are you for this?
- Have you assessed the potential cost of a major cyber event affecting UK bank operations and how this would be paid for?

Interviewees also identified the following areas where support and information would be valuable for AFB members:

- Benchmark data to assist member banks compare their cyber risk governance practices to their peers.
- Understanding best practices, for example in localised risk identification, management information reporting, and intragroup SLAs — noting the range of different contexts within which UK subsidiaries and branches operate.
- Availability of cyber awareness events for boards and management committees.
- Engagement with the PRA and FCA as to emerging approaches to subsidiary and branch cyber-risk governance so that they can reflect these in their future guidance.

Contacts

For further information, please contact:

MARSH

Charlie Netherton
CEO, UK&I Marsh Advisory and Digital

charlie.netherton@marsh.com

Jano Bermudes
Head of Cyber Risk Consulting, Marsh Advisory

jano.bermudes@marsh.com

Jamie Saunders
Strategic Cyber Consultant

jamie.saunders@marsh.com

ASSOCIATION OF FOREIGN BANKS

Andrew Brooke
Director, Policy & Regulatory Affairs

secretariat@foreignbanks.org.uk

The Association of Foreign Banks: Building Banking Business

The Association of Foreign Banks was established in 1947. Our membership includes some of the world's largest banks; their UK firms and affiliated organisations. Foreign banks make a significant contribution to London's standing as a major international financial centre and to the depth and breadth of the Global Financial Markets, facilitating global trade. Foreign banks in the UK between them oversee more than £3.5Tr: over half of all PRA-regulated capital.

Our commitment to our members is to add genuine value that is directly implementable Back@Bank.

www.foreignbanks.org.uk Twitter Linkedin

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK. For more information, please visit marsh.com