IT cybersecurity and risk management in post-merger integration projects

April 2021

pwc

Introduction

In a hyperconnected and digitalised world where millions of pieces of data are handled every day, cybersecurity plays a fundamental role. This field has become a key enabler in digitalisation processes, helping companies to bring value to the market and protect themselves against threats. As corporate digitalisation advances, data protection and cybersecurity also need to move forward to allow companies to advance their digital strategies.

According to the Allianz Risk Barometer 2020, cybersecurity is one of the top business risks worldwide. Not a single company or individual today is immune to the threat of cybercrime.

In a company integration project, security strategy is a key enabling factor for the joint company. Establishing a common understanding of cyber strategy and the company's cybersecurity operating model, as well as prioritising capabilities to navigate cyber risks (e.g. network security, cyberattacks, threat hunting strategies or creating a common data protection framework) should be the starting points for any integration process.

This white paper will provide insights, draw conclusions and answer some key questions, such as:

- What role does cybersecurity play in integration projects?
- What is the best approach when integrating two cybersecurity operating models?
- What are some of the main challenges and opportunities that can arise along the way?
- What are the key success factors?

All these points are based on best practice and experience we have gained over the last few years working with many leading global organisations.

The role of cybersecurity and risk management in IT M&A processes

Cybersecurity plays a crucial role in successfully integrating two companies. Poorly managed firewall implementation or inadequate data loss prevention processes can leave vulnerabilities which could be exploited by cybercriminals. Vulnerabilities like this erode shareholder trust, which may drastically reduce the value of the company and have an impact on its stock. They can also lead to interruption of operations, regulatory penalties, and personal liability among board members.

The dual role of cybersecurity and risk management in a post-merger integration project

During the integration process, security and risk management come under two major pressures:

- Protect: keep the company protected with the highest possible standards of security. This includes daily activities such as protecting the company from cyberattacks (e.g. ransomware and phishing), protecting sensitive company data or taking action to respond to any cybersecurity incidents identified.
- Implement and integrate: once a decision has been made on the type of integration (full or partial), the joint company needs a consistent target operating model (TOM) and framework for cybersecurity. These decisions will also form the basis for the integration programme, which will be strongly influenced by previous implementation plans of the two companies being integrated. This programme is composed of multiple projects in different areas (e.g. cyber defence, access management, IT security, risk assessment) and will serve as an implementation guide. Due to the high pressure to constantly adapt to new threats, additional requirements for cybersecurity programmes are likely to accumulate over time. It is therefore important to clearly define the scope of the integration project and organise a structured procedure for handing over follow-up activities to the line organisation.

The cybersecurity team will be involved in these tasks for some months, making it necessary to carefully organise the available resources in order to avoid creating unnecessarily stressful situations and prolonging the integration work for longer than needed. In many cases, support from an external subject-matter expert with in-depth experience will be needed.

Our approach to cybersecurity and risk management in IT M&A processes

A typical integration project consists of four main phases:

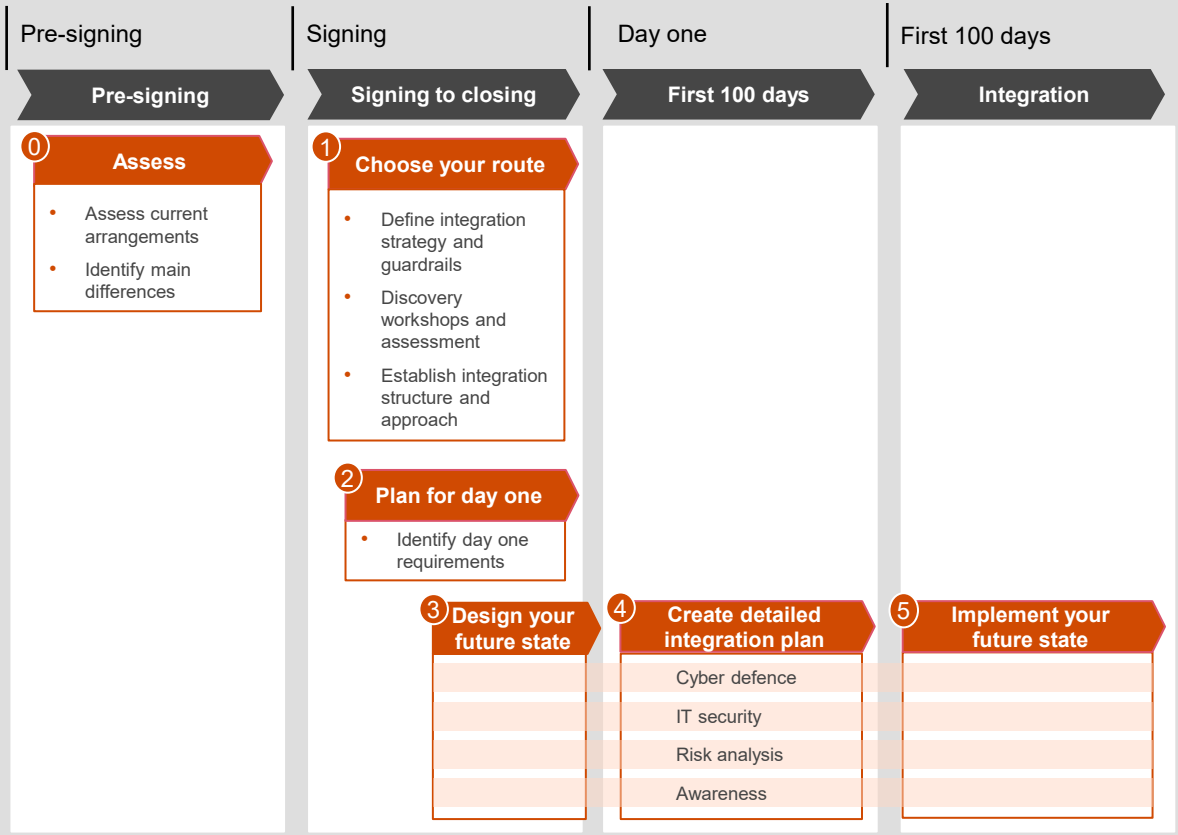
- Pre-signing
- Signing
- Day one
- First 100 days

The four phases are divided into six steps, which are explained in this chapter.

0 | Assess

Before the signing phase, you need to assess the current cybersecurity arrangements of the two companies and identify the main differences between them (e.g. cloud-based vs. in-house, ring-fence vs. endpoint protection) as part of the pre-deal due diligence process.

Phases of cybersecurity integration



1 | Choose your route

Once the purchase and integration of the two companies have been announced, you'll need to draw up a guide for the entire integration process. Our experience has shown that this will involve the following activities:

Integration process guide



Define integration strategy and guardrails

- Will the purchased company be fully integrated or only partially integrated? Will it be a combination? (best of both worlds)? What impact will this have on the current security strategy?
- Which company is most at risk of being attacked? Which has more cloud capabilities?
- Are there any legal or governmental barriers or obstacles regarding data protection and transmission of data to other countries in the country where the company being purchased is based?

Discovery workshops and assessment

Strategy

- What are the current cyber strategies of the two companies?
- Which IT security principles has each company selected for running its security function (e.g. perimeter approach vs. zero trust framework, agility vs. standardisation, centralised vs. decentralised approach)?
- How big is the budget for each aspect of security? Are there parallel and similar initiatives in both companies where we can save work and money?
- What strategies do the companies have for third parties and vendors?

People

- How many employees are working on the security landscape?
- Who are the key experts in each area?
- How motivated have they been since the integration project was announced? Is there a risk of brain drain or knowledge not being transferred?

Security processes

- What are the security processes supporting the security strategies?
- What focus do the two companies have regarding security in the workplace? Is the focus more on protection of traditional or non-traditional endpoints (i.e. cloud systems)?
- Does the security structure allow quick implementation of security projects (e.g. business information owner, information security managers)?
- Is there an imbalance of protection between the two structures that requires immediate action?

Security tools

- What are the main applications and tools used by each company (e.g. antivirus, threat hunting, data protection, vulnerability management, prevention)?
- What scope do these tools have and what are the licensing costs?
- Depending on the degree of standardisation in each company, your approach to security policy may vary considerably. Which policies will be introduced to the company being acquired (e.g. bring your own device)?

Establish integration structure and approach

- How can we structure and implement the integration plan among two cybersecurity landscapes?
- What are the main aspects of security? What will the scope of each aspect be?
- Which key internal factors affect cybersecurity (e.g. resources, technical expertise)?
- Which key external factors affect cybersecurity (e.g. infrastructure)?
- Who will lead each area of integration? Where do we have the most expertise or knowledge to lead the project?

2 | Plan for day one

Once you've set the context and assessed the current state of cybersecurity in the two companies, it's time to identify key elements you need for day one. The complexity and scope of this exercise will vary depending the results obtained during the evaluation phase. Useful questions to guide this process include:

- If some users are to be treated as regular external/guest users during the initial phase, are any adjustments necessary to ensure that they have access to sensitive information (e.g. R&D, finance)?
- Does the company need to meet any special security requirements? Are there any regulations that require higher levels of data protection (e.g. for access to sensitive data or transferring data to another country)?
- Which security applications and platforms are essential for particular groups of users to continue normal operations?

An approach to working on the main areas of a post-merger cybersecurity integration programme*

* Approach based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework

3 | Design your future state

Before you can define the target state for the joint company's security organisation, you need to complete a number of preliminary steps. These include establishing guardrails, assessing the existing security situation in the two companies, and establishing an integration approach which considers the requirements for day one. Once these steps have been completed, you'll need to take the following into account when defining your target state:

- Set an equal level of IT security and protection for both companies (security parity). This will prevent vulnerabilities in your future cybersecurity operating model when implementing initiatives
- Essential platforms and tools to protect the company from external threats (e.g. cybercriminals) and internal threats (e.g. employees losing critical data)
- Security requirements from other countries that will have a major impact on your future security organisation
- Special areas within the company that have different infrastructure setups, requiring extra work and/or with extra security requirements (e.g. R&D, manufacturing/production)
- Current information security services catalogue
- Your current situation regarding internal resources, external suppliers and your budget

4 | Create a detailed integration plan

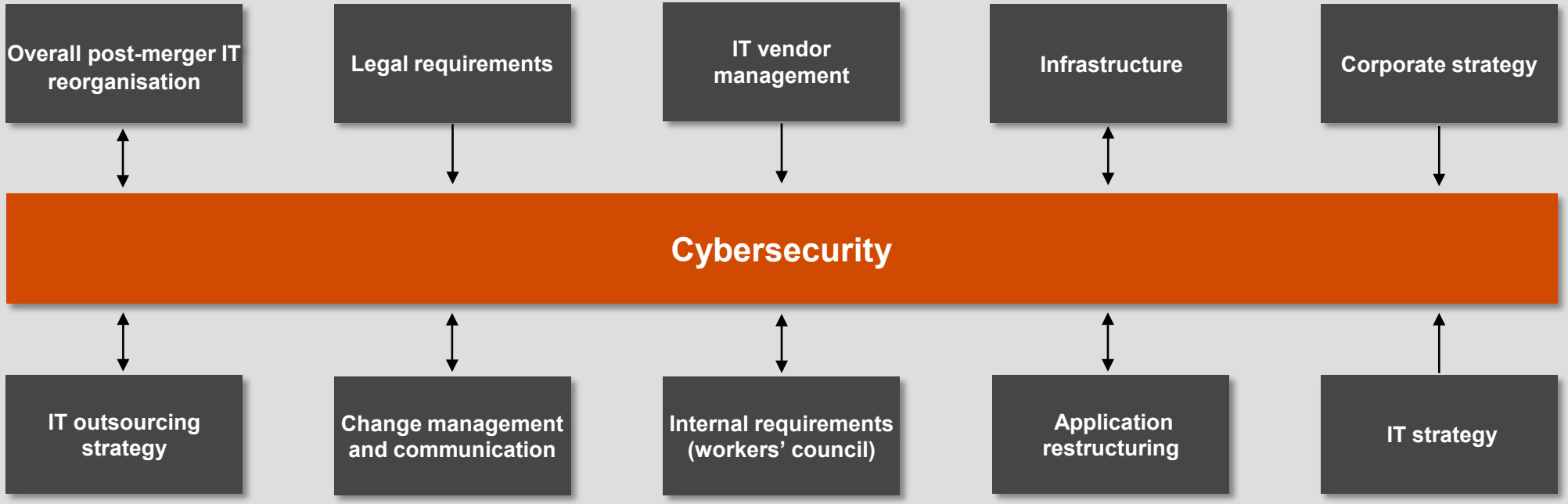
The integration plan will be your main source of guidance for reaching your target state. This is an essential document, based on traditional project management methods and approaches, and it must take into account existing project management processes in the company (scope, assumptions, roadmap, milestones, risks, budget etc.).

Cybersecurity is one of the work streams within an integration programme with a wide variety of interdependent elements. This is due to the fact that cybersecurity imposes requirements on the implementation plans of other work streams where security policies need to be applied.

There are two kinds of interdependent relationships that need to be considered:

1. Issues where cybersecurity is dependent on other areas (e.g. workplace strategy in infrastructure).
2. Projects where cybersecurity is responsible for establishing and enforcing requirements in other projects/domains in order to maintain an adequate level of security. The diagram below shows some areas where alignment and understanding are needed.

Example of key factors affecting and affected by cybersecurity



5 | Implement your future state

Once your integration plan has been created and approved, it's time to proceed with the implementation phase. During this phase, challenges and opportunities will arise and will require attention from the cybersecurity leadership team. In this phase, it's very important not only to save money or reallocate resources, but also to deal with situations that may be particularly challenging for the team. The diagram below summarises the challenges and opportunities that we have found to be most important in this phase:

Challenges

Workers' council

The entity responsible for maintaining privacy and protecting employee rights needs to be involved when implementing end-user analytics and behavioural tools (e.g. data protection, deactivating USB devices, user behaviour analytics).

Old legacy budgets

Having a clear picture of the amount of money invested in licences and services in each company is crucial – cyber security may not be always a money-saving area.

Resources

After a merger has been announced, it's to be expected that there will be organisational staff adjustments. You need to ensure that knowledge is transferred and that processes are properly documented.

Opportunities

Duplicate applications

Deactivating and eliminating duplicate security applications is a good opportunity to reduce your cybersecurity running costs.

Licences

If the company needs more licences, integration offers a good opportunity to negotiate better prices with the various providers.

Legal requirements

If the integration programme involves a country from another continent, it is likely that additional legal requirements will have to be met. In some cases, these requirements may have a positive impact by forcing the purchasing company to globally increase security on various fronts (e.g. manufacturing security).

Key success factors for cybersecurity and risk management

The diagram below summarises some key points which – in our experience – are fundamental for the integration of two cybersecurity landscapes. In most cases, help from outside experts will be required due to the complexity involved and resources necessary for successful integration.

Evaluate your team

Integrating security tools and processes will require not only security experts, but also project management skills. Make sure this is accounted for within your team, and hire in external expertise if it isn't. The following issues may be challenging within your team:

- Personal issues: when a company makes an acquisition, it is to be expected that there will be movement of people within the new company (layoffs, changes of roles, creation/elimination of positions, early retirements, new recruits, etc.), although this will vary depending on the type of merger. Make an assessment of your team and take into account their personal situations, motivations and expectations. We recommend carrying out a team risk assessment and taking adequate measures.
- Low availability of experts: this issue is related to the point above. Ensure that you have enough expertise within your team; in most cases, external support will be needed. Another point to consider is the capacity of these experts, whether internal or external. We recommend planning the time that the experts will invest in each project and prioritising work. Relying on a small number of experts can delay implementation and cause unexpected cost increases.

Evaluate your team (continued)

- Lack of project management skills: cybersecurity teams are often filled with many experts in different fields, who usually focus on one specific topic. While it is true that some of these experts will have project management skills, most cybersecurity organisations lack qualified people who can see projects from a broader, cross-functional perspective. Make sure you have people on your team who can advance the integration programme in a professional way and who know how to deal with objectives, milestones, roadmaps, risk management, reporting at different levels etc. In our experience, professional external support is essential to effectively complete the integration programme.
- Lack of clarity regarding the future cyber team structure: postponing the introduction of a new structure for your cyber team for too long can lead to many problems. These might include insecurities within the team, brain drain, delays in implementation due to lack of agreement among experts, lack of ownership, disparities when selecting security tools or processes, duplication of work and lack of motivation, among others.

Management of interdependent elements

Cybersecurity is only one part of a post-merger integration programme. During the integration phase, many projects will be running in parallel and they may affect implementation. Projects can typically be divided into three categories:

- Within the field of cybersecurity: security strategy, your future operating model and availability of resources will dictate which projects need to be deployed first. It might be that having a well-established security monitoring solution is much more important than having a behaviour analytics tool deployed. Security and privacy legislation in the countries where the company being acquired is operating is another point to consider: this can have a major impact on your integration plan. You'll need to carry out a thorough analysis of this issue and evaluate its possible consequences.
- Projects relating to other integration programmes such as:
  – IT infrastructure (e.g. workplaces, identity and access management)
  – IT organisation (e.g. new organisational models, staff restructuring)
  – change management and communication (e.g. organisation of security training sessions; deployment of new security tools that affect end users, such as data loss prevention tools).
- Other transformation programmes: in large enterprises, there will be many projects and initiatives running in parallel with the integration programme. These might include new sourcing strategies, digital transformation projects, IT cost reduction programmes, or initiatives and agreements with global providers. This category also includes workers' council negotiations and alignment, as mentioned above.

The following diagram summarises some helpful guidance for dealing with interdependent projects.

Helpful guidance for dealing with interdependent projects

TOM	Before looking at what is happening outside the field of security, you need to have a clear understanding of the future target operating model (TOM) for your security organisation. The TOM should consider how to turn strategy into operational plans: this will serve as a guide when talking to and engaging with other stakeholders throughout the company.
CISO	At a higher level, your chief information security officer (CISO) needs to know about both the future and current project portfolios running in the joint company, as these will be relevant to and have an impact on the integration programme – e.g. outsourcing strategy, vendor management processes.
Security contact	A member of the security team must be present in projects where cybersecurity needs to be taken into account (e.g. workplace, cloud transformation). They should be involved in regular meetings and they must voice their concerns whenever security requirements are not properly considered.
Cybersecurity integration lead	The programme lead should actively involve other integration project leads, organise workshops and clarify the main touchpoints – RACI matrices are highly recommended for this purpose. This will clarify issues such as who is responsible for what, or who needs to be involved in a particular meeting. You should also assess whether regular programme lead meetings are necessary (e.g. on a weekly or monthly basis).
Communication	Communicate the above points within your team and ensure that you have a common understanding across all team members.

Involve the workers' council from an early stage

Employee security and privacy is not only the responsibility of the cybersecurity team, but also of the workers' council. This is particularly relevant in European countries, where workers' councils and data privacy groups can reject or block the implementation of certain security tools. In an integration project, both parties need to go hand in hand when implementing new security solutions. Poor communication and lack of understanding may cause security initiatives to be delayed or cancelled. This can cause great frustration within your team and loss of time and money for the company. To avoid this, we recommend taking the following steps:

- Involve the workers' council from the very beginning – i.e. as soon as you have a draft of a new solution and you know which tool your team wants to implement or integrate into your future security systems. Allow enough time to get feedback from the workers' council – members are normally involved in various different management meetings, and the council needs time to evaluate and decide.
- Examine the countries where you are going to implement new solutions. Identify the countries which have a veto (i.e. which could halt the project in the country) and the countries where only an alignment is needed.
- Make just one or two cyber team members responsible for one-on-one negotiations. Begin by identifying the key stakeholders, and understanding the process and timeline. During the meetings, it's essential that the information provided is as non-technical as possible. Clearly present the benefits of the new tools and what the consequences might be if they are rejected. Depending on the workers' council approach and the number of solutions to be implemented, it may be better to get each solution approved separately rather than trying to approve all of them at the same time.

Budgeting, procurement, and cost and value management

When two IT organisations are fully integrated, it is to be expected that there will be cost savings due to duplication being eliminated (e.g. in data centres). However, this is not necessarily the case with security. If the two companies do not have security functions and platforms set up in the same way and with equal maturity, new processes and tools will need to be implemented in the joint company. This may require the company to purchase a greater number of licences and services, which will be considered non-synergies or dis-synergies.

Our experience has shown that taking some of the following steps can resolve many misunderstandings when dealing with this subject:

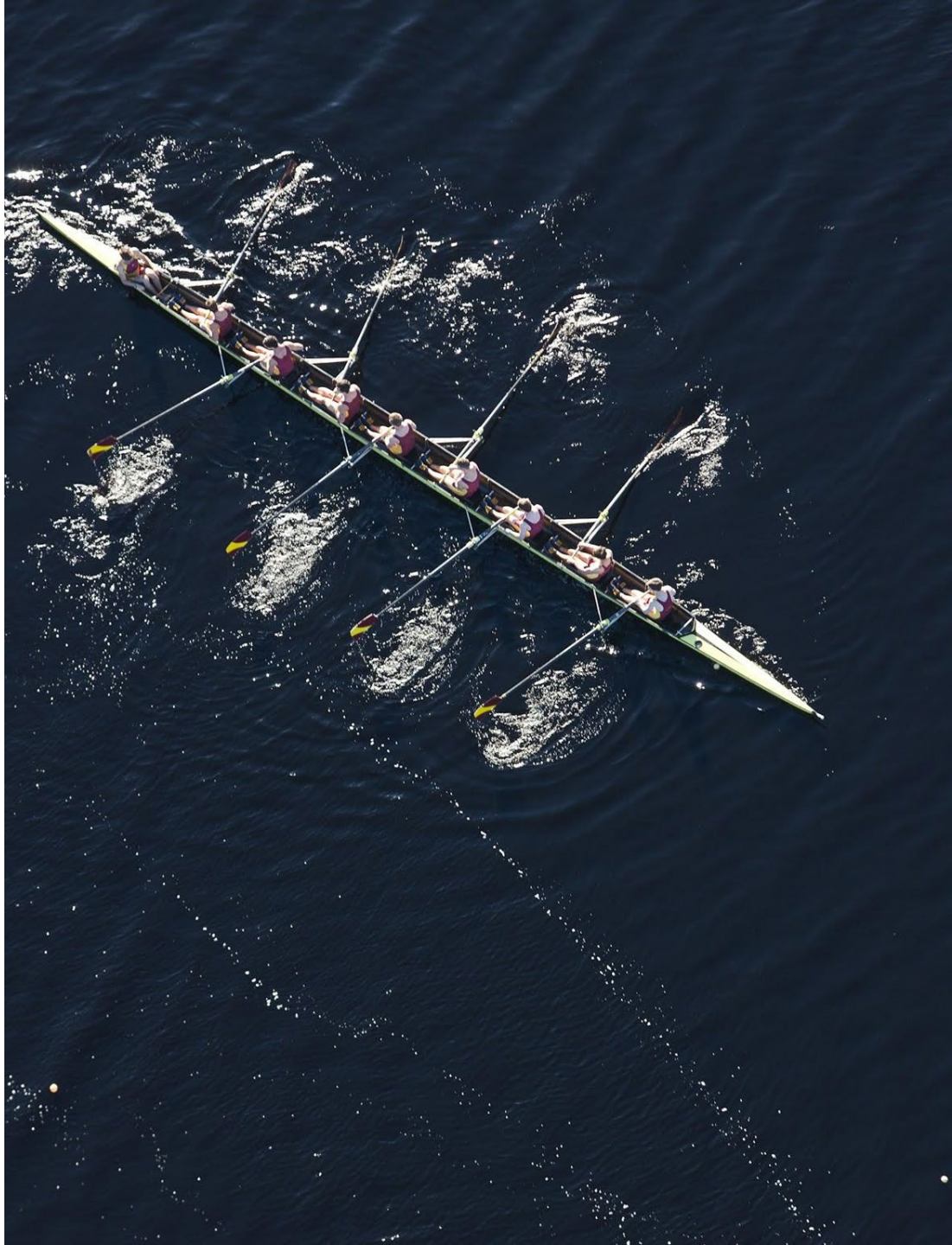
- If you have separate teams tracking budgets and costs (e.g. cost and value management, procurement, project management), make sure they all have the **same understanding** of the definition of capital expenses (CapEx) and operational costs (OpEx). This simple exercise can avoid serious misunderstandings and further alignments.
- Before integration starts, undertake an **exhaustive evaluation** of the operating expenditure (OpEx) being made on licences and services for the various tools available in the two environments. Combine those with overlapping capabilities and look for synergies to save costs and get better prices from suppliers. To do this, you'll need to get the responsible members of the procurement team and the cost and value/finance team involved.
- If possible, dedicate one person solely to **track the team budget**. They should be part of the project management team and have an overall view of invoices, payments, duration of contracts etc. Ideally, each member of the team should get approval from the budget monitor before making any purchases and/or payments.
- When tracking savings (or non-savings), you need to understand not only **how much** money will be saved, but also **when** savings will be made.

Do not underestimate the cultural context

In an international business environment, cross-cultural understanding is a key success factor for integration projects. The responsibility for this lies with the programme leader, who needs to recognise the different cultural contexts of each team member, especially at the beginning of the integration programme.

Recommendations for bridging cultural divides include the following:

- Carry out training courses and/or workshops focused on bridging gaps in understanding between different cultures within your team.
- If possible, it's better to have face-to-face meetings (especially at the beginning of the project), as direct contact will help to build trust between team members.
- Organise non-work activities to encourage contact with other members.
- Using graphics as well as words to communicate is the best way to make yourself understood across cultural barriers, especially when dealing with complex technical issues.



Contacts

Jose A. Bocarando

Senior Associate

Email LinkedIn

Manuel Seiferth

Senior Manager

Email LinkedIn

About us

Our clients face diverse challenges, strive to put new ideas into practice and seek expert advice. They turn to us for comprehensive support and practical solutions that deliver maximum value. Whether for a global player, a family business or a public institution, we leverage all of our assets: experience, industry knowledge, high standards of quality, commitment to innovation and the resources of our expert network in 155 countries. Building a trusting and cooperative relationship with our clients is particularly important to us – the better we know and understand our clients' needs, the more effectively we can support them.

PwC. More than 12,000 dedicated people at 21 locations. €2.3 billion in turnover. The leading auditing and consulting firm in Germany.

Further information:

PwC white paper series: Cyber security - protecting data and applications from unauthorised access

www.pwc.de