Government Commercial Function

COMMERCIAL AND SUPPLIER MANAGEMENT APPROACH TO MITIGATING AND PREVENTING LEGACY IT

Guidance Note

March 2022

Contents

Introduction

This guidance supports the Digital, Data and Technology Playbook.

Legacy IT is a multi billion pound problem for the government. A significant number of all new DDaT proposals are for solving legacy issues.

Government services and products must be fit for purpose. To achieve this the government needs to prevent future legacy IT and mitigate existing legacy IT. To prevent legacy IT from building up further, you need to make sure there are always clear and flexible requirements built into contacts upfront, and that contracts are managed throughout their timeline with preventing legacy IT in mind.

The Declaration on Government Reform, signed by the Prime Minister on behalf of Cabinet, and by the Cabinet Secretary on behalf of the Permanent Secretaries, stated “we will invest in the latest technology, and replace legacy IT systems that are overly complex and difficult to use” (Section 3. Performance, point 4). It also stated the need to make sure that “no new IT systems are created without interoperability with other relevant government systems” (Section 5. Annex, action 20) . How to fit new technology into your organisation is covered in the Technology Code of Practice, Integrate and adapt technology. The commitment is to invest in the latest technology, and replace legacy IT systems that are overly complex and difficult to use.

Defining legacy IT and its consequences

Legacy IT can refer to your organisation's IT infrastructure and systems, their component software and hardware, and related business processes. It becomes legacy because of any or all of the following points. The technology now is:

- considered an end-of-life product
- out of support or on extended support from the supplier
- impossible to update
- no longer cost-effective
- now considered to be above the acceptable risk threshold

Legacy IT can impact:

- cyber and national security - systems might contain old software and hardware vulnerabilities posing security risks. For example, the 2017 WannaCry ransomware attack affected health services with an estimated cost of multi millions of pounds
- operational resilience and continuous improvement - legacy IT can impact critical systems and cause errors or failure to deliver services. For example, critical systems delivering several billions of pounds in grants had operational failures due to legacy IT
- digital transformation - incompatibility between legacy and newer systems can slow down the development of new services and opportunities for automation and innovation in IT. For example, some critical national infrastructure and digital services do not use their full functionality due to legacy dependencies
- value for money - legacy IT can increase maintenance costs. For example, some specialist skills become more scarce so are charged at a premium, and manual workarounds and replacement hardware also increase costs

Commercial policies and guidelines to help mitigate and prevent legacy IT

Use the following policies and guidelines to help mitigate and prevent legacy IT.

Policies:

1. Reduce legacy IT with your business case and contract management.
2. Keep technology up to date throughout your contract.

Guidelines:

1. Understand what suppliers have available when scoping requirements.
2. Make sure you provide detailed plans to suppliers.
3. Use any IT cost savings to start resolving other legacy IT issues.
4. You should only consider a direct award if there is a compelling case.
5. Consider using outcome-based contracts to share risks and rewards with your supplier.
6. Consider how to include future-proofing in your contract and take into account new developments in technology.
7. Make use of management tools to reduce legacy IT and deliver efficiencies.
8. Make sure your supplier manages and reports on risks and issues.
9. Make sure the supplier maintains records of digital and data assets.
10. Make sure the supplier uses open standards and formats.
11. Make sure the supplier follows government technology and service standards.
12. Updating or exiting your contract and mitigating identified risks.

Policy 1- reduce legacy IT with your business case and contract management

You will need to assess your department's legacy IT to prioritise which items you need to address first. For example, departments should prioritise legacy IT with the greatest security and business vulnerabilities.

From the start of preparing a business case and contract planning, you must take into account and include the costs and time needed to address the risk of future accumulation of legacy IT. For example, keeping the software versions up to date and upgrading hardware. Subsequently, during the lifetime of the contract and any extensions, it is recommended you do not reduce or trade away these cost and time elements to gain a short term saving. This will lead to an accumulation of legacy IT at a later date which will cost more to resolve.

What to include in the business case

In addition to costs and time to address or reduce the risk of legacy IT, consider:

- dual running costs when moving to new systems
- asset lifecycle costs
- decommissioning time and costs
- partial close-down of services no longer required
- build in innovation so that technology is kept up to date

For business cases to mitigate legacy IT, consider proceeding with a longer return on investment (5+ years) and allow for a potential lack of short-term benefits to reflect the longer-term challenges of legacy IT. The business case should also recognise the wider range of benefits associated with Legacy IT remediation. For example, securing departmental service delivery, enabling future transformation, ability to attract staff and avoidance of costs caused by legacy IT.

You can find more information about what to include in your business case in The Green Book by HM Treasury.

Policy 2 - keep technology up to date throughout your contract

You should make sure all contracts include the supplier's obligation to ensure all software are supported versions and meet your requirements, throughout the contract and any contract extensions. This includes any software upgrades, updates and new releases. You should also make sure any deviations are agreed by your Contracting Authority in writing.

Getting this right at the beginning of the contract process, and throughout its life, will:

- prevent legacy IT from building up
- safeguard against risks such as cyber attack
- enable operational resilience
- allow for digital transformation
- provide better value for money

What to consider when scoping your requirements

Guideline 1 - understand what suppliers have available when scoping requirements

To proactively address risks of future Legacy IT, you should collaborate with IT suppliers to make sure that sourcing plans, IT strategy and associated roadmaps are informed by available supplier product and/or service plans. From the start, it is important to understand future development plans that align to your services evolution.

Guideline 2 - make sure you provide detailed plans to suppliers

You should communicate your IT strategy, strategic plans and enterprise architecture to potential suppliers so they can inform you of the implications for current or possible future Legacy IT.

To support this, Commercial should work with Chief Digital and Information Officers (CDIOs) to make sure the IT strategy has sufficient detail to inform a strong long-term sourcing plan.

How to fund legacy IT remediation

Guideline 3 - use IT cost savings to start resolving other legacy IT issues

You should consider the use of seed-funding and self-funding. For example, instead of cashing in cost savings, departments would ring fence this money to fund legacy IT remediation. We recommend early involvement with Contracting Authority financial teams and HMT as appropriate.

Recommendations when contracting for legacy IT remediation

Guideline 4 - you should only consider direct awards when there is a compelling case

You should only consider direct awards when there is a compelling case and only after taking legal advice. Examples of circumstances when you might use a direct award include instances when departments are ‘locked-in’ and the cost and time needed to change suppliers would be prohibitive. You will determine whether suppliers should be incentivised to ‘transform’ rather than just ’maintain’ the current service and/or infrastructure they provide.

Guideline 5 - consider using outcome-based contracts to share risks and rewards with your supplier

Where appropriate, you might use outcome-based and gain share contracts for Legacy IT remediation. Sharing risk and reward on Legacy IT remediation projects and using outcome-based contract mechanisms can provide a way to address legacy. You will need to bring suppliers into these discussions early in the process and find a mechanism to ensure value for money if you choose to implement single source or risk/reward contracts.

Future-proofing against legacy IT

Guideline 6 - Consider how to include future-proofing in your contract and take into account new developments in technology

Include suitable future-proofing measures such as:

- making sure that Intellectual Property is owned by the party best able to use it
- evergreen provisions in contracts - for example, include the necessary clauses in the contracts to make sure the relevant software is a currently supported version
- supplier risk management and reporting must include the status and risk mitigation for current software and end of life software
- asset management to include all digital and data assets
- ability for data extract and sharing capabilities - for example, suppliers should share data in open formats and provide thorough documentation
- KPIs relating to legacy mitigation and remediation
- use of government technology and service standards

Also consider future compatibility within your infrastructure and with your other services and whether you will be tied into specific contracts.

Important activities during the run stage of the contract

Once you have agreed a contract with your supplier, you will need to manage your contract and make sure that contractual provisions are completed by your supplier. For example, benchmarking, asset management, evergreen provisions and cost reduction.

Manage your contract in line with policy 2

You should make sure the supplier ensures all software are supported versions and meet your requirements, throughout the contract and any contract extensions. This includes any software upgrades, updates and new releases. You should also make sure any deviations are agreed in line with contractual and Contracting Authority governance.

Guideline 7 - make use of management tools to reduce legacy IT and deliver efficiencies

You should consider using IT demand management and cost optimisation tools to:

- identify and eliminate underused resources
- regularly match system usage to your needs
- manage teams to encourage cost savings
- avoid unintended spend (‘bill shock’) with analytics and infrastructure monitoring

Log and manage your legacy IT risks

Legacy IT risks are often not suitably quantified, managed or reported consistently. Not fully understanding them results in insufficient priority given to the remediation of the high-risk services.

Guideline 8 - make sure your supplier manages and reports on risks and issues

You must make sure your supplier uses risk management and reports on the status of the current and possible future Legacy IT for those parts of your IT estate under your supplier's management.

The supplier's reports must include:

- any identified cyber and national security risks associated with legacy IT
- independent reviews of the risk mitigation status
- the status of compliance with the contractual provisions in relation to 'evergreen' clauses

You must confirm that the supplier's risk management and reporting is overseen by at least one member of the supplier's UK Management team with digital, data and cyber expertise.

Know what technology you have, how it interacts and how it can adapt to future demands

You will have included asset management, the requirement for data extraction and sharing capabilities and the use of government technology and service standards in your contract. You will need to manage your contract and make sure these contractual provisions are implemented by your supplier.

Guideline 9 - make sure the supplier maintains records of digital and data assets

You must make sure the supplier uses best industry practices throughout the life of the contract to maintain an up-to-date view of the digital and data assets (asset inventory, configuration management database) for those parts of HMG's IT estates under their management. This should cover all:

- hardware
- software
- data
- systems and services (and their interoperability)

Guideline 10 - make sure the supplier uses open standards and formats

You must make sure the supplier provides capabilities in line with CDDO and GDS guidance for data extraction and sharing with the Contracting Authority for those parts of your IT estate under the supplier's management. For example, there is a list of open standards mandated or recommended for government use. By making sure your supplier is using open standards and formats, you will improve the interoperability of your system and its potential for reuse by other departments.

Guideline 11 - make sure the supplier follows government technology and service standards

You must make sure the supplier takes appropriate steps to future-proof new digital and data (IT) systems under the supplier's management in accordance with HMG DDaT technology policy and guidance issued by the CDDO and GDS, such as the Technology Code of Practice, Service Standard and the API technical and data standards. Examples include:

- making sure system specifications allow the possibility of code reuse
- pushing for low code solutions for software to allow for faster and more flexible software management post deployment
- your supplier using REST APIs to make it easier to move and share data

Plan changes to your contract or your exit strategy

Guideline 12 - Updating or exiting your contract and mitigating identified risks

Leave plenty of time to plan what updates you need to make to your contract, or to plan for a new contract. As referenced in the Sourcing Playbook and the Commercial Pipeline, you should aim to make published commercial pipelines look ahead 3 to 5 years to be truly effective, and 18 months as a minimum. This will help you to avoid extended or re-tendered as-is contracts which can lead to the build up of legacy IT. Use the opportunity to transform or modernise your IT. Make sure you're familiar with your controls process, for example, the Cabinet Office Controls process for departments.

If you've followed the policies and guidelines above, then you are well placed for a smooth exit from your contract. Remember to plan for dual running if a system is being replaced. Make sure you know what assets and services you have, and the impact of turning it off. Finally, close down what you can, or migrate to newer technology, in a timely manner leading to a simplified, legacy-free IT landscape and the opportunity for cost savings .