

**Report of investigation into the November
2025 *Economic and fiscal outlook*
publication error**

December 2025

Foreword

Following the premature access secured by external users to the Office for Budget Responsibility's (OBR's) *Economic and fiscal outlook (EFO)*, shortly before the Chancellor's speech on Budget day, we were asked by the OBR's Chair, Richard Hughes, to oversee an immediate investigation. We have now sent the report on this investigation, detailed below, to the Chancellor of the Exchequer and the Chair of the Commons Treasury Committee. It describes, to the best of our understanding, how this event occurred, together with recommendations to the OBR as to how to prevent any future such occurrence.

The investigation we have overseen has been led by Laura Gardiner, Chief of Staff at the OBR, ably assisted by our technical advisers, Professor Ciaran Martin of the University of Oxford and Huw Stephens, Chief Information Officer at the Treasury. We are extremely grateful to them, and to staff at the OBR, for giving their full and open support to this investigation. In assisting the preparation of this report, Professor Martin has compiled a chapter of technical findings. An annex contains our terms of reference.

All concerned have worked tirelessly over long hours to complete this report within the timescales set for us. With such a complex issue, the report is inevitably incomplete and subject to correction. Our most important conclusions and recommendations are those relating to the further work that now needs to be undertaken by others.

We are in no doubt that this failure to protect information prior to publication has inflicted heavy damage on the OBR's reputation. It is the worst failure in the 15-year history of the OBR. It was seriously disruptive to the Chancellor, who had every right to expect that the *EFO* would not be publicly available until she sat down at the end of her Budget speech, when it should, as is usual, have been published alongside the Treasury's explanatory *Red Book*. The Chair of the OBR, Richard Hughes, has rightly expressed his profound apologies.

It is also important to note that the *EFO* contains market-sensitive information, i.e. information that is not public and could have a material impact on financial markets. This is why, in the run-up to the delivery of the Budget, any leaks concerning the OBR's forecasts, whether accurate (as in this case) or inaccurate, whether inadvertent (as in this case) or deliberate, are to be greatly deplored. They must be taken very seriously by institutions from which leaks emerge. As evidence of the seriousness with which the OBR takes this issue, we have noted that throughout the preceding months the OBR had stuck rigidly to the principle of confidentiality. It is beyond the scope of this report to assess what specific factors exerted what degree of influence on the financial markets on the morning of the Budget, but we are confident that the OBR will co-operate with the Financial Conduct Authority with respect to any information it might seek.

The account of events below, and Professor Martin's technical chapter, give as full an account as it was possible to provide in the short space of time available. Professor Martin is clear that this was not a case of intentional leakage. Nor was it a simple matter of pressing the publication key too early. Those involved all believed that the protections against attempts to access the document early offered by the system were indeed in place. As Professor Martin says, *"given the absence of any obvious premature disclosures of OBR documentation in the past, this was understandable"*.

However, these protections were not in place. This is because, as Professor Martin explains, they were not applied properly and these weaknesses appear to have been pre-existing. The outcome was that the protections did not work, and efforts to secure premature access were easy to accomplish because entering a predictable internet address gave access to the document.

Professor Martin's brief look at the OBR's other online security arrangements gives some reassurance that this weakness is confined to its online publications presence, not its entire IT network. As he points out, the fact that the OBR became fully integrated into the Treasury's IT systems in December 2023 helps protect communications between the Treasury and the OBR, for which security is essential during the long run-up to the publication of *EFOs* and Budgets. The website remained locally managed to preserve real and perceived publication independence.

Access to documents on the website was only relevant to the security of the *EFO* in the final few hours before publication. Pressure on the small team involved to ensure that the full *EFO* – a substantial document – and many associated spreadsheets and other documents would be available immediately after the Chancellor sat down had led to the use of a pre-publication facility, a commonly used device that however created a potential vulnerability if not configured properly. The security of this brief phase in the production of the *EFO* had not, over the years, received the same amount of attention by the OBR as the ongoing necessity of ensuring security of communications with the Treasury during the long period of run-up to the Budget.

The ultimate responsibility for the circumstances in which this vulnerability occurred and was then exposed rests, over the years, with the leadership of the OBR. The OBR is a small analytical organisation with resources that reflect its size. The twice-yearly task of publishing a large and sensitive document is out of scale with virtually all of the rest of its publication activities. Professor Martin notes that protocols for the *EFO's* publication *"reveal a well-planned but significantly underpowered operation[...]more akin to that used by a small or medium-sized business (which of course in size the OBR resembles)"*. Responsibility for addressing this challenge by either changing the method of publication or substantially increasing the resources devoted to it rested over the years with the leadership of the OBR but also with the sponsoring department, the Treasury, and the Cabinet Office.

It is of concern that Professor Martin finds that it is very likely that the weaknesses that caused the premature accessing of the November 2025 *EFO* were pre-existing. Indeed, it appears that the March 2025 *EFO* was accessed prematurely on one occasion, though there is no evidence of any activity being undertaken as a result of that access, and he concludes the most likely explanation is benign. But it is essential that a more detailed forensic digital audit of some of the most recent fiscal events is undertaken to establish, in so far as is possible from the data, whether these outstanding

issues about the proper application of pre-publication procedures previously gave rise to other cases of premature access.

As we were asked to ensure that this investigation was conducted as quickly as possible, some of the recommendations in this report as to future arrangements will require further detailed consideration. But their direction is clear. To rebuild trust, the leadership of the OBR must take immediate steps to change completely the publication arrangements for the two important and time-sensitive documents containing the results of its biannual forecasts that it publishes in a normal year, and review arrangements for all other publications.

A straightforward solution would be to move the entire OBR online publishing operation onto the same arrangements as many other independent bodies, by moving to the government's independent subdomain, where the government provides the digital architecture but the independent body publishes what it wants, when it wants. Another option would be to hand publication of the biannual *EFOs* to the Treasury, but only if the necessary safeguards for real and perceived independence could be put in place. There may need to be an interim solution, followed by a carefully considered ultimate approach. Whatever decision is taken, new arrangements must be put in place in good time for the Spring 2026 *EFO*.



Baroness Hogg



Dame Susan Rice

Non-executive members of the Office for Budget Responsibility

1 Background and context

Background on the OBR

- 1.1 The Office for Budget Responsibility (OBR) was established in 2010 to provide independent and authoritative analysis of the UK's public finances. Its remit is set out in the *Budget Responsibility and National Audit Act 2011*. The OBR fulfils this remit in practice by publishing a range of core reports, principally its biannual *Economic and fiscal outlooks (EFOs)* which set out the economic and fiscal forecasts, published on dates set by the Chancellor alongside Budgets and Spring or Autumn Statements.
- 1.2 The OBR is led by the three members of the Budget Responsibility Committee (BRC) – currently the Chair Richard Hughes, Professor David Miles and Tom Josephs. They have executive responsibility for the core functions of the OBR. The OBR's governance, risk management and internal control are overseen by its Oversight Board, which consists of the three members of the BRC plus the non-executive members, currently Baroness Sarah Hogg and Dame Susan Rice.
- 1.3 The OBR's budget has risen gradually over the years as its staff and responsibilities have expanded, and is currently £6.4 million.
- 1.4 The BRC is supported in its work by the OBR's permanent staff of 52 civil servants, led by the Chief of Staff. The vast majority of these staff work on forecasting and analysis, aside from six who work in the 'strategy, operations and communications' team. This team covers all non-analytical aspects of the OBR's work including coordination and delivery of: finance operations and reporting, HR, and IT (which are all partially contracted to the Treasury as part of the corporate services provided within Treasury Group through a memorandum of understanding); office, estates and facilities management; press, public and other enquiries; communications and stakeholder engagement; document production and project management; and operation and maintenance of the OBR's website, social media, and other publishing functions.
- 1.5 General IT services (including email, internal document repositories, etc.) moved onto a segmented part of the Treasury's shared systems in December 2023 in order to align more closely with Treasury security arrangements, particularly around the handling and sharing, including between the two organisations, of sensitive Budget information. Previously, IT services had been provided on secure government systems by the Ministry of Justice, with which the OBR currently shares office accommodation.
- 1.6 All organisational risks, including those relating to IT, information security and website, are discussed at Oversight Board meetings, which take place three or four times a year. At each

of these meetings OBR staff present an updated risk register. These registers have consistently included risks in relation to online publication and information security, although the former has focused on the key-person risks around the external web developer, and the latter around the security of sensitive information passing between the OBR and the Treasury in the weeks and days leading up to a Budget or fiscal event. This reflects the fact that the primary concern of the OBR's leadership has been the security of information on iterations of the forecast, or the development of government policies, over the period of several weeks in which both are finalised via a highly iterative process between the two organisations.

The OBR's approach to online publication

- 1.7 Unlike all other IT systems and services, the OBR's website is locally managed and outside the gov.uk network. This is the result of an exemption granted by the Cabinet Office in 2013. After initially rejecting an exemption request, the Cabinet Office judged that the OBR should be granted an exemption from gov.uk in order to meet the requirements of the *Budget Responsibility and National Audit Act*. The case for exemption that the OBR made at the time centred on the need for both real and perceived independence from the Treasury in the production and delivery of forecasts and other analysis, in particular in relation to the need to publish information at the right time.
- 1.8 Since then, the OBR has managed its own website at the domain obr.uk. This website runs on WordPress, an open source, free-to-use content management system, hosted by WP Engine, a standard WordPress host. This type of architecture reflects good practice for an organisation with very limited resources. The website is largely a repository of published information in PDF, Excel, HTML and other formats, now containing a library of thousands of statutory reports, papers and other documents that the OBR has published over its 15-year history.
- 1.9 OBR staff run the OBR's website, including updating material and uploading newly published reports and other documents. The exception is (usually) three days per year – the days when the two *EFOs* and the summer *Fiscal risks and sustainability report* are published – when the amount of information that needs to be uploaded and the other responsibilities of the team mean an external website developer provides support with website updating and document upload. This web developer has been providing this service to the OBR throughout its history. The web developer also helps with any website development for new pages, accessibility requirements or functionality, as needed. Several re-designs have been made to the OBR's website over its existence, with a focus on improving usability and accessibility.
- 1.10 *EFOs* and supporting Excel spreadsheets and other documents (usually 20-30 in total) are published, simultaneously with the Government's Red Book, as the Chancellor sits down from his or her Budget statement. The timing of this is not known to the OBR in advance. OBR staff follow the live broadcast of the Chancellor's statement and manually publish upon hearing a few sentences at the end of the speech shared with them earlier that

morning. The *EFO* and the range of supporting documents are in high demand as soon as published, with large spikes in visits to the OBR's website. It has been the view of the OBR leadership over the years that ensuring immediate and widespread access to the *EFO* and supporting documents is of the utmost importance on the day. As a result, the OBR has set up processes that prioritise speed of access at the right time, including pre-loading of these several documents in the back-end of the website shortly (typically one-to-two hours) before they are likely due to be published. This is common practice for publication processes of this nature. The only challenges the OBR has previously faced around *EFO* publication relate to the website struggling to cope with spikes in demand, although scheduled increases in server capacity on *EFO* publication days mean that this has not been a problem in recent years.

- 1.11 In the course of this brief investigation, we looked at the publication plan for the November 2025 *EFO*, which was entirely typical of the approach to previous *EFOs*, and we talked to the key personnel involved. Two things are apparent. One is that the plan, and the resources behind it, while well-developed, were fragile in relation to the magnitude of the task, reflecting the OBR's size and budget. The second is that those involved were working on the basis that the underlying technology used by the OBR ensured that pre-publication uploads were not generally accessible. The assumption was that even though the URL could be guessed because it followed a clear pattern from previous *EFOs*, the protections provided on WordPress would ensure it could not be accessed.
- 1.12 Relevant audits by the Government Internal Audit Agency, and regular website testing by OBR staff, have focused on testing and improving website accessibility and performance. These did not identify the events that took place on 26 November as a risk.

Timeline of events on Wednesday 26 November

- 1.13 The key message from those involved in the publication of the *EFO* and associated documents on 26 November was that the same process that had been followed on previous Budget or fiscal statement days was followed in the same way, up until OBR staff became aware that the *EFO* had been accessed early via the OBR's website. The sequence of events was as follows:
- 05:10 – the website host emailed OBR staff to confirm that server modification to accommodate higher website traffic at the time of *EFO* publication was complete.
 - 05:16 – website activity logs show the earliest request on the server for the URL https://obr.uk/docs/dlm_uploads/OBR_Economic_and_fiscal_outlook_November_2025.pdf. This request was unsuccessful, as the document had not been uploaded yet. Between this time and 11:30, a total of 44 unsuccessful requests to this URL were made from seven unique IP addresses.

- 09:00 onwards – the web developer set up webpages (no PDFs, Excel spreadsheets or other documents were uploaded during this stage) in draft form in the content management system, creating IDs for all the downloads to be used across the website.
- 11:02 – PDF documents were emailed to the web developer, including the *EFO* document.
- 11:03-11:53 – the other supporting documents and files were sent to the web developer. 25 files were to be published in total.
- 11:30-11:35 – the web developer began uploading documents to the draft area of the OBR website (which was understood by all involved to be not publicly accessible), including the *EFO* PDF.
- 11:35 – the first successful request to the internet address (URL) https://obr.uk/docs/dlm_uploads/OBR_Economic_and_fiscal_outlook_November_2025.pdf was made. The IP address of this first successful request had made 32 previous unsuccessful attempts at this URL over the course of the morning. There were a total of 43 requests to this URL that were successful between this time and 12:07, from 32 unique IP addresses.
- 11:41 – the first evidence online of the *EFO* being publicly available, via a Reuters news alert entitled 'UK OBR ECONOMIC AND FISCAL OUTLOOK: BUDGET TAX RISES RAISE 26.1 BLN STG BY 2029-30'.
- 11:43 – an OBR staff member was first made aware by a (non-Reuters) journalist that Reuters was flashing extensive forecast details.
- 11:43 – OBR staff attempted to rule out the OBR website as the source. Not knowing that the URL for the *EFO* PDF was accessible even if known or guessed, the focus was on whether the relevant parts of the website had been pushed live accidentally, or whether there had been a leak of the document not connected to the publication process. OBR staff found no evidence via the front-end of the website that webpages had gone live accidentally.
- Around 11:50 onwards – images of and facts from the *EFO* began appearing widely online from many people (suggesting the PDF had been widely downloaded, and/or shared by other means after download).
- 11:52 – senior OBR and Treasury officials telephoned each other to discuss the breach. These Treasury officials made OBR staff aware of the URL leading to the PDF of the *EFO* that was accessible.
- 11:53 – OBR staff and the web developer attempted to pull the PDF from the website, and also to pull the entire website (e.g. via password protection), but struggled to do so initially due to the website being overloaded with traffic.

Background and context

- 11:58 – an email was received to the OBR press inbox from a Reuters journalist confirming that Reuters had published details of the *EFO* and asking for comment.
- 12:07 – the *EFO* PDF was renamed by the web developer.
- 12:07 – the *EFO* PDF appeared on the Internet Archive. This means it was, at that precise time, visible entirely generally on the open internet via search engines. It is assumed that this happened very briefly in the rush to remove it.
- 12:08 – the *EFO* PDF was removed from the website’s content management system, taking it offline.
- 12:08 – the OBR Chair and staff drafted a statement setting out briefly what had happened and confirming that the OBR’s website was the source of the error.
- 12:15 – this statement was posted on the front page of the OBR’s website, and on X (formerly Twitter).
- 12:34 – the Chancellor’s Budget statement began, opening with a reference from the Chancellor to the early release of the OBR *EFO*.
- 13:38 – the Chancellor’s statement ended and the *EFO* and supporting documents were immediately pushed live.
- 16:29 – the online version of the *EFO* PDF was updated with a correction slip at the front, after approval of these corrections by the House of Commons Journal Office.

2 Technical findings

The technical background

2.1 The OBR website logs and its security operations centre data have been made fully available to the investigation team. This is the basis of the technical conclusions in this report. As the timeline in the previous chapter establishes:

- The *Economic and fiscal outlook (EFO)* was accessible between 11:30 and 12:08 for anyone with access to the internet address, or URL (and appears to have been more broadly discoverable for at least a very small part of this time as it was cached by the Internet Archive at 12:07 – it is assumed that this happened briefly and accidentally in the rush to remove the page).
- During that period, it was accessed 43 times by 32 unique IP addresses.
- The first access was at 11:35. This came from an IP address which had attempted to connect to the URL of the *EFO* on some 32 occasions on that day. In all, seven different IP addresses tried to connect to the URL before 11:30, with 44 unsuccessful attempts in total.
- The first evidence that the *EFO* was publicly available came at 11:41, when Reuters published a news alert entitled ‘UK OBR ECONOMIC AND FISCAL OUTLOOK: BUDGET TAX RISES RAISE 26.1 BLN STG BY 2029-30’.
- The *EFO* PDF was removed at 12:08.

2.2 For those 38 minutes, access to the *EFO* was possible for anyone who could guess the URL of the publication and type it into an address bar of a web browser. That is not the only way it could have been accessed in advance, and it is possible that some of the accesses were via the OBR’s website directory. Once it becomes known that a URL is accessible, it is easily shared (for example, if the recipient of a WhatsApp message with the URL clicks on the link, the document will load). Therefore it is unsurprising that the document was accessed on multiple occasions once the URL was known.

Technical background to and causes of the error

2.3 Detailed reports from the security operations centre confirm the absence of any hostile cyber activity, or any malfeasance from within the OBR. Furthermore, there is a clear and obvious explanation for what happened, which is a combination of two technical errors in

Technical findings

configuring the tools and digital infrastructure needed to keep a pre-publication document private until its intended publication time.

- 2.4 Pre-uploading publications in advance is standard practice in many organisations. This means that the document is on an organisation's website, but is not generally accessible, at least through the normal methods of: (a) clicking on a highlighted link from the hosting organisation's website; (b) using a standard search engine; or (c) typing in a URL.
- 2.5 For low-risk, non-sensitive publications, organisations and individuals sometimes use this approach to share advance copies of a document. This allows trusted users to view something in advance. It is highly insecure, of course, because any sharing of the URL means access to the document.
- 2.6 This practice is therefore not appropriate for higher-risk and sensitive publications, so organisations in this position can use various techniques to ensure that the benefits of pre-uploading the document in advance are realised without giving general access. One effective way of doing this is to obfuscate or obscure the URL by giving it a long sequence of random characters that are essentially unguessable. Another way protection can be added is by requiring a password until publication, or some other form of authorisation of access.
- 2.7 Such features are commonly carried out by what are known as content management systems – services used by organisations to manage online publications. WordPress, one of the most widely used of such systems, is used by the OBR, hosted by WP Engine. A web developer – a supplier – handles some content upload and other matters. For the purposes of content upload, WordPress has a commonly used feature for handling scheduled publications to keep what it calls 'future' content hidden. It works off authentication, rather than the obfuscation of the URL. The OBR team worked on the assumption that because they were using this service, as they had done for many years, the recent content was being treated as 'future' and was therefore hidden. Given the absence of any obvious premature disclosures of OBR documentation in the past, it is understandable that this was the assumption.
- 2.8 However, content management systems, like other key systems, will not function as intended if they are not configured absolutely correctly. Technical commentary has, for many years, noted that WordPress can be onerous to configure and that mistakes are easily made in so doing.
- 2.9 In the context of this rapid investigation, it has become clear that two mutually contributory configuration errors were made in the OBR's use of pre-publication features. One is the configuration of WordPress. A feature known as the Download Monitor plug-in created a webpage with the clear URL which provided a link to the live version, which bypassed the need for authentication. This rendered the protections on the 'future' function of WordPress redundant as it bypassed the required authentication needed to gain access to the pre-uploaded document. The creation of a URL in the clear is a feature of the plug-in which requires specific mitigation if it is not to lead to the document unintentionally being visible before publication. This was obviously not understood within the OBR's online publishing

function so the Download Monitor plug-in should not have been used in this way without that understanding. The available mitigation is at server level and prevents access to download or file storage directories directly. If configured properly, this will block access to the clear URL and return a 'forbidden' message. This is the second contributory configuration error – the server was not configured in this way so there was nothing to stop access to the clear URL bypassing protections against pre-publication access.

- 2.10 In short, the technical causes of the premature access were two mutually contributory configuration errors, one in the configuration and use of Download Monitor, a third-party WordPress plug-in, and one in the configuration of WordPress and the underlying server.

The origins of the problem and previous *EFOs*

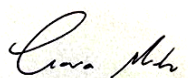
- 2.11 In the course of reviewing last week's events, it has become clear that the OBR publication process was essentially technically unchanged from *EFOs* in the recent past. This gives rise to the question as to whether the problem was a pre-existing one that had gone unnoticed.
- 2.12 In the short time available, we have only analysed the traffic for the March 2025 *EFO*. The correct time of publication would have been 13:06, when the Chancellor finished speaking. Public records indicate that that is when it appeared on the OBR's website in the normal, generally accessible way. However, the logs show that one IP address successfully accessed the document at 12:38, five minutes after the Chancellor had started speaking and nearly half an hour before publication. It is not known what, if any, action was taken as a result of this access and there is no evidence at this stage of any nefarious activity arising from it.
- 2.13 It has not been possible in the time available to establish definitively where this IP address came from (and there are robust restrictions in law on investigative powers around IP addresses in any case). There are some indications the IP address may be linked to accounts within UK government and/or other public authorities within the UK.
- 2.14 There are potentially many entirely benign explanations for what happened in March 2025. At the time of finalising this report all the indicators pointed to a benign explanation but the investigation had not yet fully concluded. Therefore, no conclusions should be drawn from this finding other than it seems to prove that the configuration problems that gave rise to last week's events were in existence for the March 2025 *EFO* also, even if they did not lead to the same outcome. It is this finding that gives rise to the recommendation that a fuller forensic digital audit of recent *EFO* publications is undertaken to probe this further. As a start, what happened in March 2025 requires further examination, and it would be prudent to examine the logs for the two previous *EFO* publications from 2024, if possible.

The OBR's publication process

- 2.15 In 2013, the OBR secured an exemption from the central government requirement for all public authorities to use the gov.uk domain. This was an important decision aimed at bolstering the then new organisation's demonstrable independence from the Treasury and

the rest of government. The 2013 decision means the OBR runs its online publications entirely separately from the rest of government, where there is an integrated and standardised approach. The OBR website is widely used and is seen as well-designed and user-friendly.

- 2.16 The OBR does not, however, run its other IT systems independently of government. Its data storage, email systems, and so on, are shared with the Treasury and other parts of Treasury Group. This is the same arrangement as for most other independent bodies within the public sector. So any of the weaknesses identified in this investigation in terms of IT and data procedures apply only to published documents, rather than sensitive internal discussions within government. There are therefore no wider implications arising from this episode in terms of vulnerability to, for example, state espionage on sensitive governmental deliberations in advance of fiscal events.
- 2.17 Despite its considerable influence and expertise, the OBR is, in organisational terms, very small, with a budget appropriate to a small analytical organisation. Examination of the OBR's plans for publication of the November 2025 *EFO* and multiple related documents reveal a well-planned but significantly underpowered operation. The technology stack and the configuration methods used on the OBR website are some of the most widely used globally, but the tier of product deployed is more akin to that used by a small or medium-sized business (which of course in size the OBR resembles). One simple example of this that emerged during the investigation is the remarkably small file size to which the OBR is limited in publishing. Moreover, enterprise solutions might have embedded audit or review processes which would catch the sort of configuration errors that caused last week's incident. Furthermore, the OBR's own risk register notes the vulnerability of its publication capability to absences of single individuals like a web developer. This is in marked contrast to the scale of the Treasury's capabilities to publish the rest of the critical Budget material, and there are numerous other examples in government of the sort of scale and capability needed to ensure successful publication of major government outputs, especially those with particular sensitivities around their publication. The OBR's online capabilities, processes and procedures are insufficient for the vital and sensitive task it is entrusted to deliver.
- 2.18 The OBR is unusual, though not unique, among independent scrutiny bodies in being entirely self-sufficient in online publishing and the maintenance of an online web presence. Many independent bodies playing crucial roles in the scrutiny of public life come under the umbrella of the *independent.gov.uk* subdomain. The overall infrastructure is managed by government, but the timing and content of publication is entirely delegated. That is why as well as considering specific new arrangements for future *EFOs*, there is another model for the entirety of the OBR's online presence which can be considered.



Professor Ciaran Martin

Professor at the Blavatnik School of Government, University of Oxford

3 Conclusions and recommendations

Causes of the event

- 3.1 There is, in the view of our expert technical adviser Professor Ciaran Martin, nothing to suggest that the failure to protect the *Economic and fiscal outlook (EFO)* from premature access during a pre-publication period of 38 minutes on 26 November was the result of hostile cyber activity by foreign actors or cyber criminals, or of connivance by anyone working for the OBR. Nor was it simply a matter of pressing the publication button on a locally managed website too early. The cause, which appears to have been pre-existing, was, in essence, configuration errors which reflected systemic issues. These led to a failure to ensure the protections which hide documents from public view immediately before publication were in place.
- 3.2 This meant that those responsible for publishing the documents believed they could not be accessed; this was not the case. As the protections did not work, the document was accessible via an internet address that was predictable because it followed a clear pattern of addresses from previous *EFOs*.
- 3.3 From the evidence gathered in this brief investigation, it is apparent that the procedures followed for the November 2025 *EFO* were the same as those for previous publications. It can therefore be assumed that there is a high likelihood that the opportunity for premature access that existed for a brief period last week was present for at least some previous *EFO* publications. In essence, therefore, this is a pre-existing issue.
- 3.4 Indeed, a brief examination of online traffic prior to the March 2025 *EFO* indicates one successful attempt to secure pre-publication access to that *EFO* five minutes into the Chancellor's Spring Statement speech on 26 March. There is no indication of any activity following this access, and at the time of going to press Professor Martin concludes the most likely explanation is benign. However, it illustrates that the problem exposed last week was not a new one. We could not, in the time available, carry out deeper forensic examination of other recent *EFO* events and **we recommend that such an exercise is, with expert support, now urgently carried out.**
- 3.5 Reliance on a locally managed website for the publication of a massive and highly sensitive document such as the *EFO* exposed the OBR, with very limited resources for the task, which led to the risk of such an incident occurring. Like all independent fiscal institutions, it was incumbent on the OBR from the start to establish its independence from government. So the organisation was granted an exemption by the Cabinet Office in 2013 from placing its website under the umbrella of gov.uk. Instead the OBR's website, its development and management, including publication of the *EFO*, was managed by the OBR itself.

Conclusions and recommendations

- 3.6 Given the small size of the organisation, the OBR used an outside web developer from a government framework to assist a small internal team with its website design and maintenance. This supplier managed content and uploads at times of pressure, which included the controlled release of major reports and papers.
- 3.7 Over the years, however, the risks associated with this approach have increased, as technologies have developed and with the rise in online threats of many kinds, and ***with hindsight, it is clear that over the years this arrangement should have been regularly re-examined and assessed by the management of the OBR.***
- 3.8 The security focus of the leadership team has been primarily on the risks posed by constant interchange with the Treasury during the period of several months in the run-up to a Budget. This risk has been mitigated by the OBR's switch to use of the Treasury's own IT services, to which there was a successful migration from the services of the Ministry of Justice (in whose building the OBR currently resides) in December 2023. ***The OBR should also undertake a full review as to whether it continues to be appropriate for the OBR to maintain its own entirely separate online publishing operation, rather than the one under the umbrella of the government's independent subdomain used satisfactorily by many other independent bodies. It should not attempt to carry out these tasks on its own, but form a working party involving the leadership of the technology and communications communities within government.***
- 3.9 Consideration of the risks associated with the much shorter period when the *EFO* was supposedly hidden in a safe space on the OBR's website prior to publication was focused on risks around publication, such as the likely surge in demand, and the key-person risk around the web developer. The assumption that pre-publication protections worked created an ongoing blind-spot. The risks had been increased by the need to make quite lengthy use of this pre-publication facility in order to ensure that the whole document could be made publicly available when the moment came for release. Adding to the difficulties, this moment could not be precisely known in advance, since custom and practice determined it should be at the moment when the Chancellor sat down. ***We recommend that the process for publishing the EFOs (normally two times a year) should immediately be removed from the locally managed website and conducted in an environment more appropriate to the nature of the task (see below).***

Consequences of the event

- 3.10 The *EFO* contains much market-sensitive information, normally not in the public domain until the Treasury *Red Book* of explanatory material is also published.
- 3.11 It is not within our competence to say what market movements between 11:30, (when the document was uploaded in pre-publication form but was unintentionally accessible) and 13:38 (when the Chancellor concluded her Budget statement) were affected by the achievement of early access to *EFO* material. We note however that those who secured early premature access did, at least, disseminate it quickly and widely, through the use of such

mechanisms as Reuters alerts, rather than keep it for their private advantage. **We are confident that the OBR will cooperate fully with the Financial Conduct Authority (FCA).**

- 3.12 The number of people in Parliament and the media who had achieved access to the *EFO* before the Chancellor rose to her feet demonstrates the degree of disruption she suffered at a key point on Budget day. For the Opposition to receive this information well in advance of the normal moment changed the pattern of Budget day to the Chancellor's disadvantage. **We greatly deprecate this and believe the OBR is fully cognisant of the damage that was done.**

The way forward

- 3.13 The urgent task is to reform the way in which the twice-yearly *EFOs* are published. The OBR is, like many small organisations, under-resourced for the task, and we note the use of the single-person supplier brought in to help on such occasions as a key-person risk. **We are therefore strongly of the view that completely new arrangements should be put in place for the publication of these major market- and time-sensitive documents.**
- 3.14 A straightforward solution would be to move the OBR's online publication systems to the government's independent subdomain, where the government provides the digital architecture but the independent body publishes what it wants, when it wants. This is the approach taken by many other independent bodies. There may be other publication shelters with greater resources than the OBR in the public sector and the OBR may also want to consider an interim route of publication of the Spring 2026 *EFO* via the Treasury, notwithstanding the core requirement for real and perceived independence of OBR publications. **We believe that the security of the *EFO* is paramount, especially in Spring 2026, not least because success among those seeking premature access this time will certainly encourage future attempts.**
- 3.15 It may continue to be appropriate to treat less-sensitive OBR publications differently, even retaining a locally managed website which is highly regarded by users, if that is thought to be worthwhile. **However, as detailed above, we urge the OBR to carry out an urgent and thorough review, with external assistance, of its website protocols in order to judge which route to take for all publications.**
- 3.16 The use of Treasury IT services for everything except its website gives Professor Martin encouragement to believe that the failed protection of the *EFO* pre-publication does not indicate a general lack of security capability within the OBR. However, in the light of the rising tide of threats to online security, **we recommend that the OBR engages with a suitable external expert to review all its arrangements, and sets a regular pattern for such reviews in the future.**
- 3.17 Tension is evident between the need to limit spending on arrangements which are only put to the test twice a year, and to limit the use of scarce resources on these events, with the need to ensure adequate protection through the process. The OBR does not have an 'IT

Conclusions and recommendations

department'; responsibility is carried by a very few individuals with many other tasks to fulfil. ***We recommend that the Treasury, in setting the OBR's budget, pays greater attention to the need for adequate support to be provided and/or adequate expertise to be fully funded.***

- 3.18 This event is an object lesson in the challenges faced by small organisations to keep pace with online developments, options and threats. Although it is not our business to advise others, at the urging of our expert adviser ***we would encourage other agencies of government handling sensitive material to use this event as a prompt to review their own arrangements.***

A Investigation terms of reference

A.1 The OBR inadvertently made it possible to access the November 2025 *Economic and fiscal outlook (EFO)* too early on Budget day. The OBR issued a statement apologising and launching an investigation.¹ Below are the particulars for that investigation.

Personnel and timelines

A.2 This investigation should be conducted swiftly, in order that the Chancellor, the Treasury and the House of Commons Treasury Committee can be informed of the facts of what happened and the further actions that need to be taken in response at the earliest possible opportunity. The investigation's report should be published no later than Monday 1 December.

A.3 The investigation will be overseen by the independent members of the OBR's Oversight Board (Baroness Sarah Hogg and Dame Susan Rice). It will be supported by Ciaran Martin, Professor at Oxford University and former CEO of the National Cyber Security Centre, who will act as an expert adviser. In addition, with the support of the Treasury, it will be able to draw on the expertise of Treasury IT and security specialists.

A.4 The investigation will produce a report to the Chancellor, the Treasury and the Commons Treasury Committee which will be published.

Terms of reference

A.5 The investigation shall:

- Establish the events that made it possible to access the *EFO* early.
- Determine the actions needed to assure the Oversight Board, the Chancellor, the Treasury and the Commons Treasury Committee that no future breaches of forecast security will take place.
- Set a timeline for implementing those actions.
- Make other recommendations to the OBR in light of its findings, as it sees fit.

¹ <https://obr.uk/our-upcoming-november-2025-economic-and-fiscal-outlook/>

