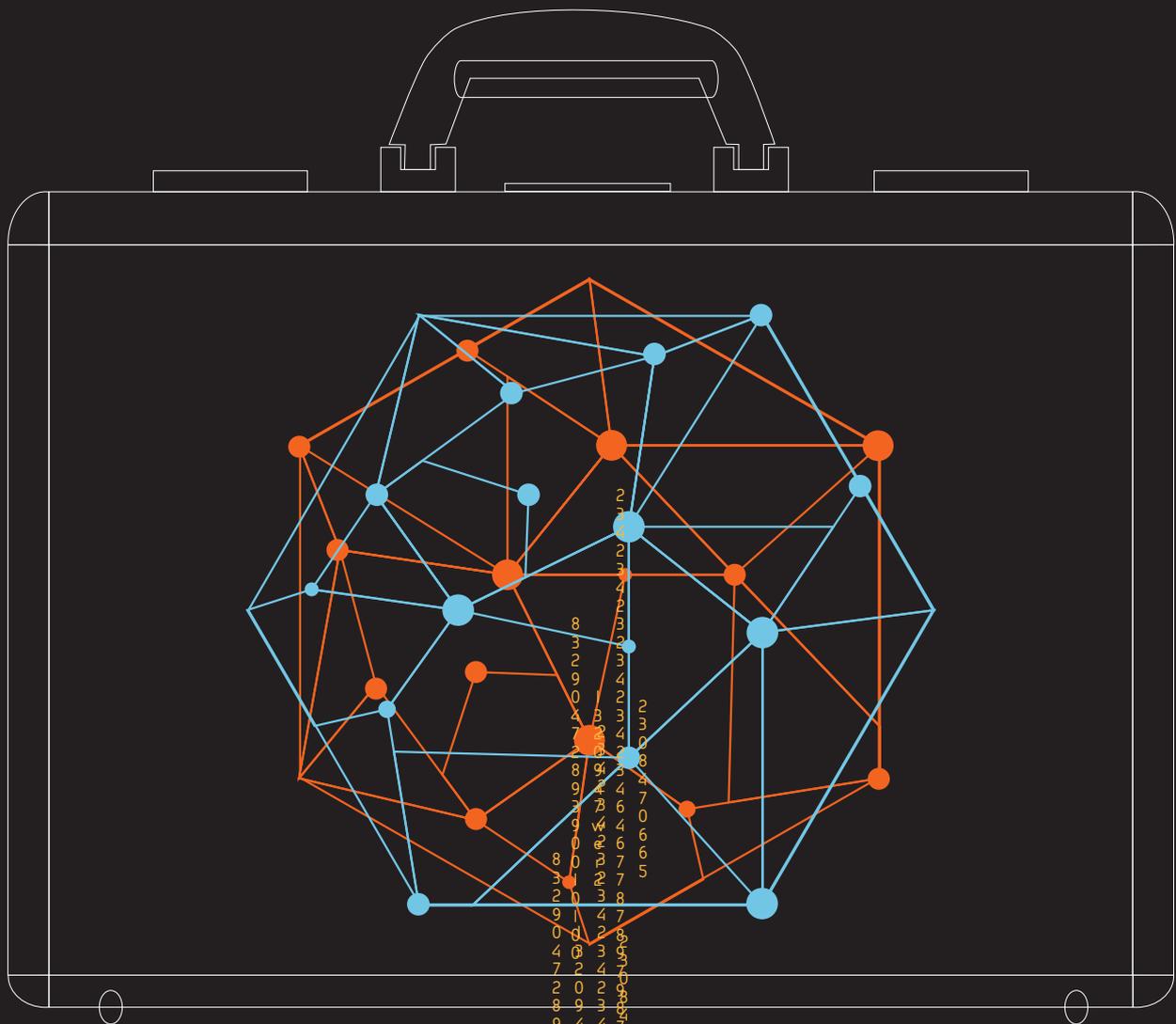


Using the cloud to solve your compliance conundrums

Build a business case for putting compliance into the cloud

BANKING INSIGHTS



BAE SYSTEMS

Using the cloud to solve your compliance conundrums

Financial institutions may have been reluctant to embrace cloud technology until now. Perhaps it was due to the supposed security risks, or maybe cost was cited as a reason for their hesitation. However, relatively quickly, those concerns have been mitigated.

If the cloud was seen as a potential risk for compliance before, today it's seen as an enabler of flexible and more efficient processes. The cloud provides better security, the ability to scale for remote working, cost control, the opportunity to make the most of your data, and much more.

In this Insight report, Brian Ferro, Global Head of AML/BSA Compliance Product Management at BAE Systems, explores why a growing number of financial firms are embracing cloud technology in order to solve the growing compliance challenges they face.

Read on and learn how you can build a business case for embracing compliance in the cloud technology

Business case point one: the need to respond to rising regulatory pressure

Over the past decade, banks have had to comply with an increasing number of regulations to guard against emerging financial crime typologies. Thomson Reuters reported that in 2019 alone, over 220 international regulatory changes occurred every day, amounting to 80,000 updates that year.¹ And it's not just the strictly enforced violation fines that are damaging to financial services firms, but also the negative impact on their reputation.

The scale of these spiralling regulatory demands – and the many systems required to run a compliance function – requires extremely robust risk management. Many firms are struggling to adhere to risk management models such as BASEL III, which impact efficiency. And there are concerns over whether the systems and processes in place are robust enough to keep pace with compliance obligations over a firm's entire landscape.

Walking the compliance tightrope is becoming trickier than ever – especially at a time when banks are working to prevent a recession. Banks are taking decisions today that will attract a lot of scrutiny in the near future. So, they need to ensure they have the rationale and a data trail to back up what they are doing.

The cloud can help organisations to meet their compliance obligations and become ready for an uncertain regulatory future. Cloud technology enables banks to handle reporting in an elastic way, as well as providing the necessary long-term data storage. They can flex and scale their computing power according to demand, and only pay for what they use – less waste, more control.

¹ [Financial crime worries rise](#), Chloe Domat, Global Finance (9 April, 2020)

Business case point two: increasing intelligence required to battle increasingly intelligent crime

Technology-enabled financial crime and fraud continues to plague the banking sector worldwide. In the UK alone, the cost for banks combating cybercrime and online fraud amounts to £6.7 billion, according to the Financial Conduct Authority.² To be future ready, institutions must move faster than the criminals who seek to attack them.

Banks are trying to deal with a changing world while maintaining business as usual. They have to adapt rapidly to the shifting profile and pace of financial crime. As fraud moves from transaction-based to identity-based attacks, banks must be diligent when making customers aware of the types of scams taking place. For example, banks were quick to educate customers about fraudsters calling and trying to get them to release funds. They now have to work hard to keep up with the increasingly intelligent and sophisticated approaches.

Data holds the key to combatting evolving financial crime tactics. But harnessing its full power and potential is far from straightforward, especially as data governance challenges begin to emerge. This is magnified when data is held on many different systems, becoming inaccessible and difficult to extract.

Through the use of high-speed advanced analytics, cloud-based solutions can enable FIs to deal with these data governance hurdles more effectively, as well as detecting fraud more accurately. This is because vast amounts of data can be processed quickly to inform decisions and deliver accurate results.



The scale of these spiralling regulatory demands – and the many systems required to run a compliance function – requires extremely robust risk management.

² [Understanding the costs of cyber crime](#), Home Office Science Advisory Council (January, 2018)

Business case point three: enabling remote employees to access data

Even before Covid-19 made working from home a normality, habits were already changing. The number of people who mainly work from home has increased in the past five years³ and that upward trajectory is expected to continue. This is in part due to changing attitudes and in part to improved network capabilities. Organisations no longer have to worry about the number of desks in the office. Cloud technology allows organisations to scale for remote working now and in the future.

At a time when organisations across the board are striving to make the most of their data and become analytics-driven, efficient analytics tools are included as standard within a cloud environment. This means that remote workers can easily and securely interrogate data in different ways.

It's important to consider the cultural and change management requirements that come with cloud-enabled remote working though. Employees will need educating on how to work safely and securely, so as not to expose the organisation.

Business case point four: cost-crunching capabilities are necessary during a recession

Cost efficiency matters more than ever as the economy enters what is predicted to be the worst recession in 100 years.⁴ FIs are under increasing pressure to become leaner and more efficient, yet the increase in regulatory requirements often means more staff and higher costs.

The increasing false positive volumes and Know Your Customer checks can drive up costs as Compliance Managers battle to maintain an effective function. At the same time, there's pressure across the industry to strip cost from non-revenue generating areas.

FinTech and RegTech innovations offer new ways to automate and simplify these processes. But, if you're running a number of disparate solutions, overall efficiency is harder to achieve.

The cloud offers a scalable model which allows organisations to move from a capital expenditure (CapEx) to an operating expenditure (OpEx) model. And because the solutions are delivered as managed services, it frees up time and resources to improve the efficiency of the overall compliance operations.

³ [Coronavirus and homeworking in the UK labour market: 2019](#), ONS (24 March, 2020)

⁴ [Economic impact of the coronavirus crisis is 'dire everywhere,' OECD says](#), Silvia Amaro, CNBC (10 June, 2020)

A complete, comprehensive cloud platform

Our fully managed compliance package, NetReveal 360°, is cost-effective, adaptable, offers industry leading security and is compatible with multiple environments. Its cloud security levels adhere to the same security standards as our government deployments, and it provides the benefits of reduced costs and complexities of maintaining an up-to-date and comprehensive compliance solution.

Discover how NetReveal 360° can help you to:

- Prevent financial crime
- Protect against cyberattacks
- Adapt to demanding compliance regulations

About the author



Brian Ferro, CAMS, Global Head of Product Management for AML/BSA Compliance

Brian Ferro is responsible for managing the direction of the Compliance Solutions at BAE Systems Applied Intelligence. He's accredited as a Certified Anti-Money Laundering Specialist (CAMS) and is a Certified Associate in Anti Money Laundering (FIBA) by exhibiting extensive knowledge of compliance guidelines and federal regulations.

Prior to joining BAE Systems, he spent four years in a similar role with another vendor and 15 years in Financial Crimes Investigations and Compliance with one of the world's leading financial institutions where he managed a Special Investigations Unit (SIU) that coordinated investigations and projects with law enforcement agencies.

Recommended content:



[READ] Five reasons why now's the time for compliance in the cloud



[DISCOVER] How cloud platforms can fortify your compliance programmes



[LEARN] More about the NetReveal 360 solution



[MEET] Brian Ferro, Global Head of Product Management for AML/BSA Compliance

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/bankinginsights

 linkedin.com/company/baesystemsai

 twitter.com/baesystems_ai

Copyright © BAE Systems plc 2020. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.