Date informal advice provided: 14 January 2025

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments

CASE STUDY:

Managing the impact of third party software defects on resilience

Response from Ofcom, FCA, ICO, and CMA

This is an anonymised version of a query submitted to the DRCF AI and Digital Hub ('the Hub').

The query in this case study has been responded to by the following DRCF regulators ('we', 'us', 'our'):

- Information Commissioner's Office ('ICO');
- Competition and Markets Authority ('CMA')
- Financial Conduct Authority ('FCA'); and,
- Office of Communications ('Ofcom').

This informal advice is provided in line with the Conditions for Participation.

Our informal advice is provided to a business based on our current understanding of the legal and regulatory frameworks within our remits and how they apply to the business's service. This informal advice should not be treated as an exhaustive account of the issues linked to a business's service or represent an endorsement of their proposed innovation.

Our informal advice is specific to a business's circumstances as described by them in the information they provided to the Hub.

Our informal advice is provided without prejudice to any future regulatory intervention by any DRCF or non-DRCF regulator and nor is it a substitute for independent legal advice which a business may wish to seek in advance of the launch their service.

It is ultimately a business's responsibility to assess their position under the law and regulatory regime, with the benefit of independent legal advice as necessary. Recognising that some regulatory regimes are still developing and could change over time, businesses have a responsibility to keep up to date with the latest position.

A non-confidential version of the informal advice provided to the applicant is attached to this case study. This informal advice was provided on 14 January 2025 and represents the position as at 14 January 2025. Businesses should consult

relevant information and guidance on regulators' websites to keep up to date with the latest developments.

Summary of query and response

- Business A operates a digital solution which uses AI to support business IT and cybersecurity by enhancing their operational resilience and preventing disruptions and outages caused by third-party software flaws. This includes both security vulnerabilities and non-security flaws in third-party software that could disrupt critical operations. It serves IT and cybersecurity departments across sectors like finance, healthcare, and telecommunications to analyse and prioritise bug reports from third-party vendors which enables IT departments to manage these operational risks proactively.
- The query to the Hub sought clarification on whether the risk management framework for operational third-party software defects should align with that for security vulnerabilities. The questions were:
    - Confirmation that third party software defects with the potential to cause outages and disruptions—whether or not they are security related—must be managed consistently in order to ensure effective resiliency and risk management practices?
    - Can the DRCF AI and Digital Hub provide or suggest appropriate sources that affirm the need to address non-security defects as part of operational resilience efforts?
- Operational resilience is an important part of maintaining financial stability in the UK. Ensuring the financial sector is operationally resilient is important for consumers, firms, and financial markets. An operationally resilient financial system can absorb and adapt to shocks and disruptions, rather than compound them.
    - Operational disruptions and the unavailability of important business services have the potential to cause wide-reaching harm to consumers which means that firms must have robust plans in place to deliver essential services, no matter the cause of disruption.
    - These disruptions include threats such as IT system outages, third-party supplier failure, and cyber-attacks.

- Resilience, and in particular, availability, is a key part of maintaining electronic communications networks and services, and digital infrastructure in the UK.
    - Network and service providers and operators of essential services in the digital infrastructure subsector are required to take appropriate and proportionate measures to identify and mitigate resilience risks.
    - This includes both "cyber-security type" compromises such as those caused by malicious actors, as well as a broad range of other types of impacts on the resilience of networks and services, such as outages caused by external factors (e.g. floods, cable cuts, or power cuts) or internal factors (e.g. hardware failures, software failures, operational process errors, or network design flaws).
- Under data protection law, organisations should proactively identify and address software defects that have the potential to compromise personal data.
- To the extent that Business A's clients are engaged in the promotion, sale or supply of products to (or from) consumers, consumer law is likely to apply to them. Depending on the specific facts of the case, consumer law may also apply to Business A where Business A's activities are directly connected with that promotion, sale or supply (even where Business A do not have any dealings with consumers).

Date informal advice provided: 14 January 2025

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments

Introduction to the regulators

This query has been responded to by the FCA, ICO, CMA and Ofcom. A brief introduction to each regulator has been included below.

Each regulator is responsible for separate legal regimes with different requirements that may be applicable to the same set of facts, and it will be necessary to take steps to comply with each regime as set out.

Ofcom

Ofcom is the regulator for the communications services that we use and rely on each day. Ofcom regulates the TV and radio sectors, fixed line telecoms, mobile, postal services, plus the airwaves over which wireless devices operate.

Communications providers and operators of essential services in digital infrastructure are required to comply with security and availability obligations. These include managing security risks, minimising impact on consumers, and reporting any security breaches or network failures to us.

As part of Ofcom's programme to enable strong and secure networks for people across the UK, Ofcom carries out various activities to oversee network security and resilience, and ensure providers comply with the rules.

Ofcom works closely with the Department for Digital, Culture, Media and Sport (DCMS), the National Cyber Security Centre (NCSC) and industry to monitor potential risks as well as providing guidance and advice to support new legislative frameworks.

Ofcom oversees the following regulations that are relevant to this query:

- Communications Act 2003
- Network and Information Systems Regulations 2018

FCA

The Financial Conduct Authority (FCA) is the UK's financial services regulator with focus on reducing and preventing serious harm, setting higher standards and promoting competition and positive change.

The FCA regulates the conduct of around 42,000 businesses and prudentially supervises around 41,000 firms.

The FCA oversees the following regulations which are relevant to this informal advice:

- Financial Services and Markets Act 2000
- Payment Services Regulations 2017

- Electronic Money Regulations 2011

ICO

The Information Commissioner's Office ('ICO') is the UK's independent public authority set up to uphold information rights. The ICO oversees the UK General Data Protection Regulation ('UK GDPR'), which is relevant to this informal advice.

CMA

The Competition and Markets Authority ('CMA') is the UK's lead competition and consumer authority and an independent non-ministerial department of the UK government. The CMA helps people, businesses and the UK economy by promoting competitive markets and tackling unfair behaviour. The CMA's ambition is to promote an environment where consumers can be confident that they are getting great choices and fair deals, and competitive, fair-dealing businesses can innovate and thrive. The CMA enforces the following laws which are relevant to this informal advice:

- the Consumer Protection from Unfair Trading Regulations 2008 ('CPR'); and
- Business Protection from Misleading Marketing Regulations 2008 ('BPRs').

The CMA's response is for indicative purposes based on the limited information available, and whether a particular practice breaches consumer law will require a case-by-case assessment based on the particular facts and circumstances. In its response, the CMA does not set out every situation or practice as part of which a breach of the CPRs may occur. Further, the CMA does not have any information regarding how Business A's services may be used by consumer-facing businesses.

Regulator Response References

In the below table, we have set out the relevant regulator and the respective responses that they have input on. Each regulator is only responsible for the responses within their regulatory remit as noted in this table.

Regulator	Question	Relevant Responses
FCA	Q1	1.2 – 1.7
	Q2	2.2 – 2.4
Ofcom	Q1	1.8 – 1.19
	Q2	2.5- 2.10
ICO	Q1	1.20 – 1.23

	Q2	2.11 – 2.15
CMA	Q1	1.24 – 1.30
	Q2	n/a

Response

1. Confirmation that third party software defects with the potential to cause outages and disruptions—whether or not they are security related—must be managed consistently in order to ensure effective resiliency and risk management practices?

1.1. Resilient infrastructure systems are seen by government as being important, not just for electronic communications and finance, but all critical national infrastructure sectors. The Cabinet Office has published the National Risk Register and the UK Government Resilience Framework[1].

Financial services

1.2. Authorised financial services firms must manage risks in software and applications through an established risk framework, process and procedures, regardless of whether they are caused by security or non-security known or unknown bugs, to ensure the availability of important business services and avoid any intolerable harm that may occur to consumers or any risk to market integrity.

1.3. The FCA has made rules in SYSC 15A of the FCA Handbook that set out the FCA's requirements and expectations on how firms that are within scope of these rules should act in the event of operational disruptions including system failures and changes to systems. This includes the requirement on firms to maintain appropriate systems and controls which includes how the firm manages its software development lifecycles and underlying systems and architecture on the software/applications that support their important business service.

1.4. The rules in SYSC 15A aim to ensure firms that are within scope of these rules are able to respond to, recover and learn from, and prevent future operational disruptions.

1.5. Firms are required to identify the people, processes, technology, facilities and information necessary to deliver their important business service under SYSC 15A.4.1R, and are expected to understand the same in relation to any service outsourced to or provided by an external third-party under SYSC 15A.4.2G. Firms are required to understand the potential vulnerabilities and where those vulnerabilities may occur, whether they sit with the third-party or beyond. Firms are also expected to work with the third party to carry out scenario testing under SYSC 15A.5.5G. This should include controls on all applications of technology that

[1] HMG, 2023. National Risk Register and HMG, 2022. The UK Government Resilience Framework

could potentially disrupt services and application around AI functions. Firms should consider vulnerabilities (security and non-security) on a continuous basis.

1.6. SYSC 15A.1.1 R sets out which firms the rules in SYSC 15A apply to, namely: banks, building societies, designated investment firms, insurers, Recognised Investment Exchanges (RIEs), enhanced scope senior managers' and certification regime (SM&CR) firms, entities authorised or registered under the Payment Services Regulations 2017 (PSRs 2017) or the Electronic Money Regulations 2011 (EMRs 2011) and consolidated tape providers.

1.7. Where firms fall out of scope of these operational resilience requirements, they should still consider any relevant sector-specific expectations communicated to them by the FCA.

Electronic communications

1.8. An important aspect of any electronic communications network and any associated services is resilience. The requirements in the Communications Act 2003 (the Act) on providers of public electronic communications networks and services (PECN/PECS) to ensure their security and resilience were recently amended by the Telecommunications (Security) Act 2021(TSA), which imposed new security duties on providers of PECN/PECS.

1.9. Section 105A[2] of the Act (as amended by the TSA) states that providers of PECN/PECS must take "such measures as are appropriate and proportionate" for the purposes of identifying and reducing the risks of "security compromises" or preparing for their occurrence. Section 105C[3] further provides that providers of PECN/PECS must take appropriate and proportionate measures to prevent adverse effects arising from a security compromise and, where such adverse effects do arise, to remedy or mitigate those adverse effects on the PECN/PECS.

1.10. The definition of a "security compromise" includes *"anything that compromises the availability, performance or functionality"* of PECN/PECS, and *"anything that causes signals conveyed by means of the network or service to be lost"*[4]. Therefore, this will include both "cyber-security type" compromises such as those caused by malicious actors, as well as a broad range of other types of impacts on the resilience of PECN/PECS, such as outages caused by external factors (e.g. floods, cable cuts, or power cuts) or internal factors (e.g. hardware failures, software failures, operational process errors, or network design flaws). These

[2] s105A(1) Communications Act 2003
[3] s105C(2) and (3) Communications Act 2003
[4] s105A(2)(a) and (d) Communications Act 2003

latter aspects are more often associated with threats to network and service availability and reliability, and accompanying protective measures to improve network and service resilience such as redundancy and capacity planning, hardware and software maintenance, hardening, and change management.

1.11. The Electronic Communications (Security Measures) Regulations 2022 set out additional specified measures or measures of a specified description that providers of PECN/PECS must take. These measures are designed to ensure that providers of PECN/PECS are following appropriate and proportionate practices. The Telecommunications Security Code of Practice also gives guidance as to the measures to be taken under sections 105A to 105D by the provider of a PECN/PECS.

1.12. Regulation 3(3)(e) requires providers of PECN/PECS to take such measures as are appropriate and proportionate in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment. Annex B of the Telecommunications Security Code of Practice includes advice on how to assess the security of network equipment in the context of the security duties imposed on PECN/PECS. This guidance is taken from the NCSC's Vendor Security Assessment (VSA) Version 1.0, which was published in March 2022. This recommends testing software maintenance, releases, version control and documentation.

1.13. Regulation 12 on "Patches and updates" also states that where a patch or mitigation is made available relating to the risk of a security compromise occurring, a PECN/PECS provider *"must take such measures as are appropriate and proportionate to deploy the patch or mitigation within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise which the patch or mitigation addresses"*.

1.14. Ofcom has produced its own resilience guidance which sets out the measures it expects PECN/PECS providers to take in relation to the availability, performance, and functionality of their networks and services. This guidance explains that software failures are a threat to resilience and should be considered by PECN/PECS providers when assessing the appropriate and proportionate measures that they need to take.[5]

Essential services

1.15. The Network and Information Systems Regulations 2018 (NIS Regulations) establish a national framework for the security of network and information

[5] See paragraph 1.3.6, Network and Service Resilience Guidance for Communication Providers

systems in the United Kingdom. The NIS Regulations designate national competent authorities [6] for a number of subsectors who are responsible for enforcing those regulations. Ofcom is the designated competent authority for the digital infrastructure subsector in the United Kingdom.

1.16. Under the NIS Regulations, operators of essential services (OES) must comply with various duties. The types of essential services falling within the digital infrastructure subsector are: Top Level Domain (TLD) Name Registries; Domain Name Systems (DNS) Resolver Services; DNS Authoritative Hosting Services; and Internet Exchange Points (IXP).

1.17. Regulation 10[7] requires OES to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies, and to prevent and minimise the impact of incidents affecting the "security of the network and information systems used for the provision of an essential service".

1.18. As with electronic communications, the "security of network and information systems" is defined broadly and includes resilience, specified as *"the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."*[8]

1.19. It follows from both the Act and the NIS Regulations, where a software defect risks the availability of a PECN/PECS or a network and information system on which an operators essential service relies, then appropriate and proportionate measures should be identified to reduce those risks.

Data Protection

1.20. Under the UK General Data Protection Regulation ('UK GDPR'), organisations must implement appropriate technical and organisational measures to protect personal data – a requirement known as the **security principle**. This principle is foundational within the UK GDPR and covers not only protections against external

[6] See page 25, Security of Network and Information Services: Guidance for Competent Authorities
[7] Regulation 10(1) of the NIS regulations states that "OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies".
Regulation 10(2) provides that "OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services"
[8] Section 1.3(g) of NIS regulations

threats but also expectations around operational resilience, which includes ensuring the **confidentiality, integrity, and availability** of personal data.

1.21. Article 32 of the UK GDPR further specifies that both data controllers and processors must secure their processing environment by minimising the personal data they collect, managing access, and protecting the **CIA triad** (confidentiality, integrity, and availability) of personal data. Organisations are also required to build resilience into their systems and regularly test the effectiveness of their security measures.

1.22. In addition to the security measures outlined in Article 32, **Article 25 – Data Protection by Design** is also highly relevant. This provision mandates that organisations integrate data protection principles into their processing activities from the outset. While not exclusively focused on security, it requires organisations to proactively identify and address potential defects or misconfigurations that could undermine the integrity of data processing systems. By designing systems with built-in protections and anticipating risks – such as those posed by software defects – organisations can prevent disruptions or data breaches, ultimately ensuring the availability and integrity of personal data.

1.23. Where a software defect – whether security-related or not – has the potential to disrupt service availability or compromise personal data, it should be managed in a way that prevents harm to individuals. This reflects the UK GDPR's risk-based approach to information security, which requires organisations to assess and manage risks with measures appropriate to their personal data processing.

Consumer Protection

1.24. Business A should also consider the potential application of consumer law.

1.25. Businesses are prohibited by the Consumer Protection from Unfair Trading Regulations 2008 (CPRs) from engaging in unfair commercial practices concerning consumers. 'Commercial practice' covers any act, omission, course of conduct, representation or commercial communication by a business which is directly connected with the promotion, sale or supply of products or services to (or from) consumers. 'Consumer' means an individual acting for purposes that are wholly, or mainly, outside that individual's business. As such, the CPRs apply to a wide range of commercial behaviour such as advertising, marketing, sales, supplies and after-sales services.

1.26. To the extent that Business A's clients are businesses engaged in a commercial practice concerning consumers, the CPRs are likely to apply to them and they are ultimately responsible for their compliance.

1.27. Even if Business A's clients are businesses, if Business A's practices nonetheless have a direct connection with the promotion, sale or supply of goods or services to or from consumers (even if they are not Business A's goods or services), then the CPRs may also apply to Business A. Whether such a direct connection exists will depend on the specific context and content of a particular practice. If this is the case, Business A must take steps to ensure that Business A's r own practices comply with the CPRs.

1.28. The CMA refers Business A to the CMA's AI Foundation Models Initial Review, particularly Sections 5 and 6 of the initial report, which set out potential consumer protection concerns about foundation models (including false and misleading outputs) and the CMA's general views on compliance with the CPRs and other consumer protection legislation (eg unfair terms law). The CMA published a set of six principles in its AI Foundation Models: Update Paper to help guide markets towards positive outcomes for UK businesses and consumers. The CMA urges all firms to align their business practices with the principles the CMA has set out. The CMA also refers Business A to the CMA's draft Unfair Commercial Practices guidance. The CMA recommends Business A keeps updated on the CMA's published AI work and draft Unfair Commercial Practices guidance as they progress.

1.29. Similarly, Business A should consider the Business Protection from Misleading Marketing Regulations 2008 ('BPRs') which prohibit Business A from giving misleading information to Business A's business clients that would deceive that business and affect, or be likely to affect, their economic behaviour.

1.30. The CPRs will be replaced by the Digital Markets, Competition and Consumers Act 2024 ('**DMCCA**'), when the relevant part of the legislation comes in force in 2025. However, the informal advice referred to in this response is likely to be substantially unchanged in practice.

2. Can the DRCF AI and Digital Hub provide or suggest appropriate sources that affirm the need to address non-security defects as part of operational resilience efforts?

2.1. The Hub has collated a range of guidance published by FCA, Ofcom and the ICO in relation to operational resilience and cyber security within their remit which supports firms to understand and meet their relevant obligations. These are listed below:

Financial services

2.2. The FCA published its policy statement Building Operational Resilience which sets out final rules in SYSC 15A on how firms within scope of those rules should approach operational resilience. The FCA has also set out rules and guidance on outsourcing in SYSC 8 (for firms) and SYSC 13.9 (for insurers).

2.3. The FCA has published guidance on Outsourcing and Operational resilience and Outsourcing to the 'cloud' and other third-party IT services

2.4. The FCA has also published its AI Update setting out its approach to AI which is focused on how firms can safely and responsibly adopt and understand AI innovations, including scrutiny of systems and processes in place to ensure regulatory expectations are met.

Electronic communications

2.5. This Secretary of State has published the Telecommunications Security Code of Practice under section 105E of the Act. This code of practice provides guidance for large and medium-sized public telecoms providers as to the measures to be taken under sections 105A to 105D by the provider of a PECN/PECS. Telecommunications Code of Practice.

2.6. Annex B of the Telecoms Security Code of Practice includes advice on how to assess the security of network equipment in the context of the security duties imposed on PECN/PECS.

2.7. Ofcom has also published various guidance relevant to providers of PECN/PECS and operators of essential services respectively.

PECN/PECS

2.8. Ofcom has published a general statement of policy under section 105Y of the Communications Act 2003. This procedural guidance provides general guidance on Ofcom's approach to exercising its functions to seek to ensure compliance with the security duties. General statement of policy under section 105Y of the Communications Act 2003

2.9. Ofcom has also produced resilience guidance which sets out the measures Ofcom expect PECN/PECS providers to take in relation to the availability, performance, and functionality of their networks and services. This replaces Ofcom's previous 2022 guidance, which itself updated Ofcom's 2017 guidance on security requirements. Network and Service Resilience Guidance for Communication Providers

Operators of essential services

2.10. Ofcom has published guidance in relation to the digital infrastructure subsector. This guidance provides a high-level introduction to the NIS regulations and sets out Ofcom's views on the steps Ofcom expect OES in the digital infrastructure subsector to take, as a minimum, to meet their obligations under the NIS regulations. **Guidance for the digital infrastructure (PDF, 831.3 KB)**

Data Protection

2.11. The ICO has produced guidance on Information Security, which confirms that personal data must be processed securely by means of appropriate technical and organisational measures. In addition, these measures must ensure the three key elements of information security; confidentiality, integrity and availability of systems, services and the personal data processed within. Any outage or disruption would render the systems, services and personal data unavailable contrary to this requirement.

2.12. In addition, this guidance confirms that organisations are also required to have the ability to ensure the resilience of their processing systems and services and explains that resilience refers to:

- Whether systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident;
- An organisation's ability to restore them to an effective state.

2.13. This includes business continuity plans, disaster recovery and cyber resilience. However, there is a wide range of solutions available and the appropriate solution will depend on the exact circumstances of a particular organisation. The ICO's guidance on AI and Data Protection may also be useful, as it addresses issues such as bias, discrimination and model errors, along with advice on how organisations can mitigate them.

2.14. ICO recommends that Business A refers to the ICO's DPIA Guidance, which provides valuable insights on the importance of assessing risks when adopting new technologies. This includes evaluating third-party software solutions, which can help identify and mitigate potential vulnerabilities, ensuring that any risks to data protection are appropriately addressed and managed in compliance with the UK GDPR requirements.

2.15. Finally, the National Cyber Security Centre's ('NCSC') has published guidance on Supply Chain Security, which provides detailed information about developing resiliency within supply chains.