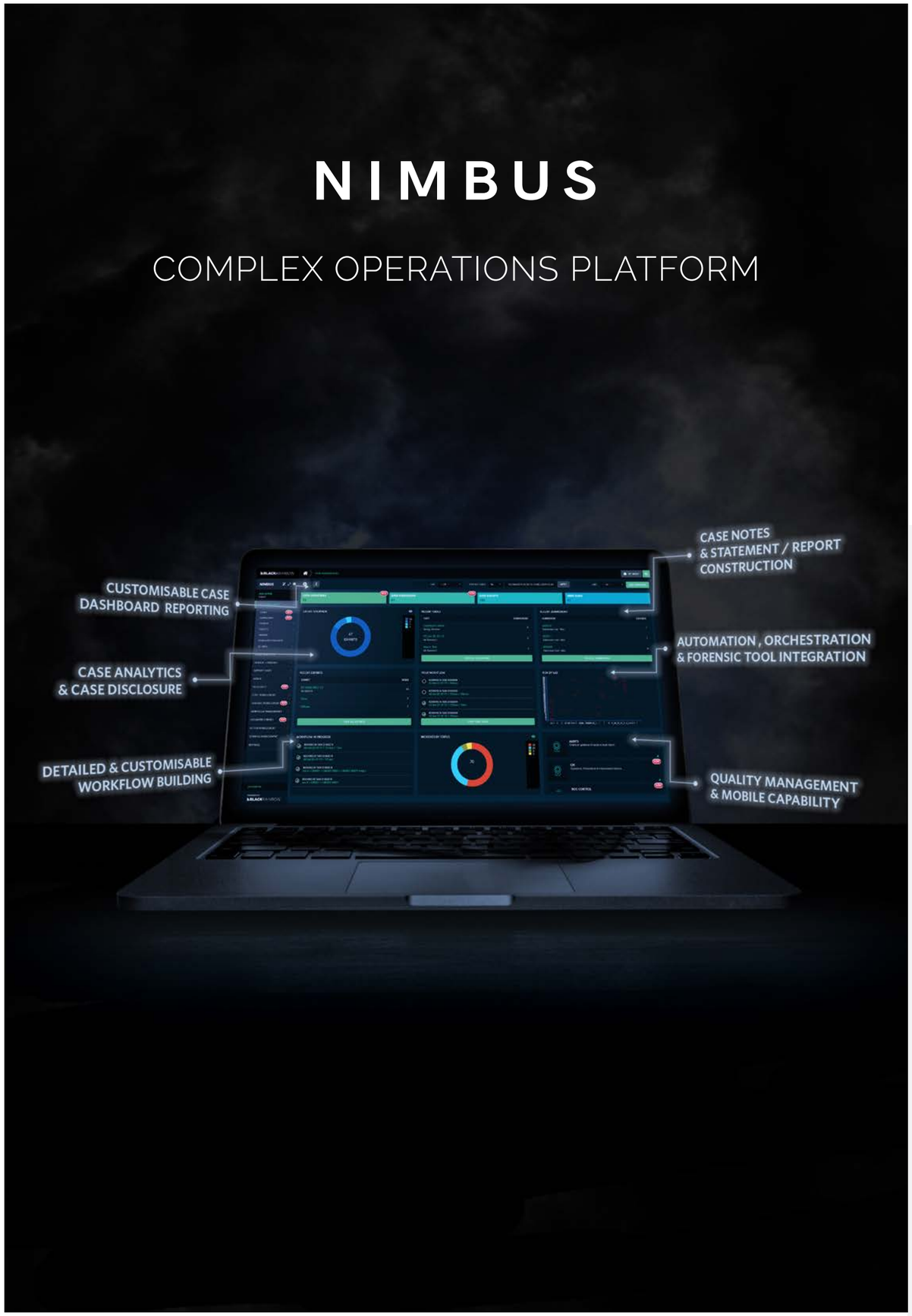
BLACKRAINBOW

7 ways NIMBUS addresses the ICO recommendations on mobile phone extractions and data management



We are proud of our ‘whole system’ data management approach

At BlackRainbow, we pride ourselves on our meticulous approach to data management and how it can be used for safeguarding the public, policing, and evidence. We work alongside our customers to fully understand the complexity of their particular issues, helping them to build effective and innovative solutions.

The recent report by the ICO clearly highlights the systemic complex challenges around the sensitivity and intrusion of mobile phone extractions. There is a real and pressing need for investigators to be able to control the processing, categorisation, disclosure, and retention of this extremely sensitive personal data.

We have years of experience and research in this field and understand these multi-faceted and complex issues. We developed NIMBUS to manage a ‘whole system approach’ and believe that it addresses many of the issues and recommendations highlighted in this report.

NIMBUS is an advanced Case and Quality Management System, accessible either locally or in the cloud as a SaaS. It manages data from collection to court and beyond, including appropriate disposal, ensuring a true ‘end-to-end’ process, with all practices managed, recorded and legally compliant.

Read 7 ways NIMBUS addresses the ICO recommendations →

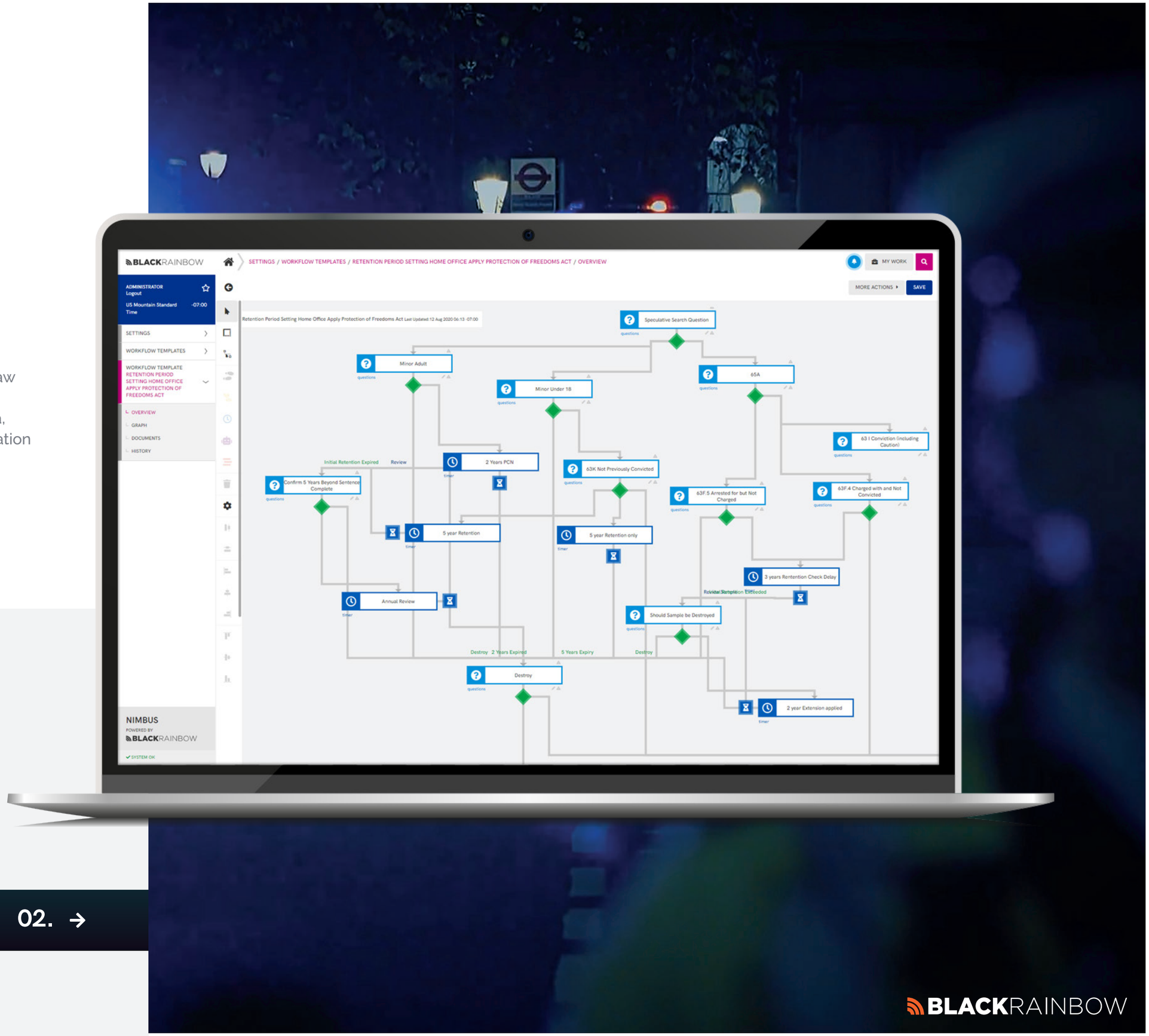
BLACKRAINBOW

01.

Recommendation 1 - 3

Legal and strictly necessary

NIMBUS workflows are designed to protect the rights of individuals by categorising data according to the law and powers being exercised, the sensitivity and ownership of the data, retention requirements and their relation to the investigation.



02. →

02.

Recommendation 4 & 5

International standards compliance and policy driven processes

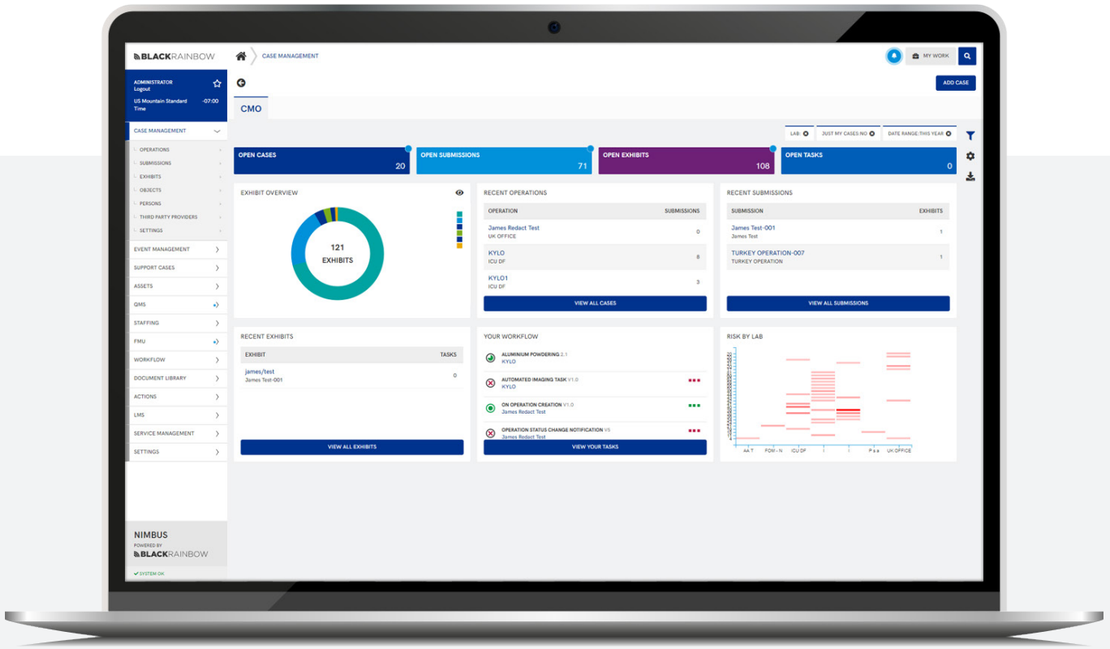
NIMBUS seamlessly integrates Case and Quality Management systems, ensuring the application of policy to operational work is controlled. This includes the prevention of any tasks where the correct level of competence, asset control or authorisation is not present.

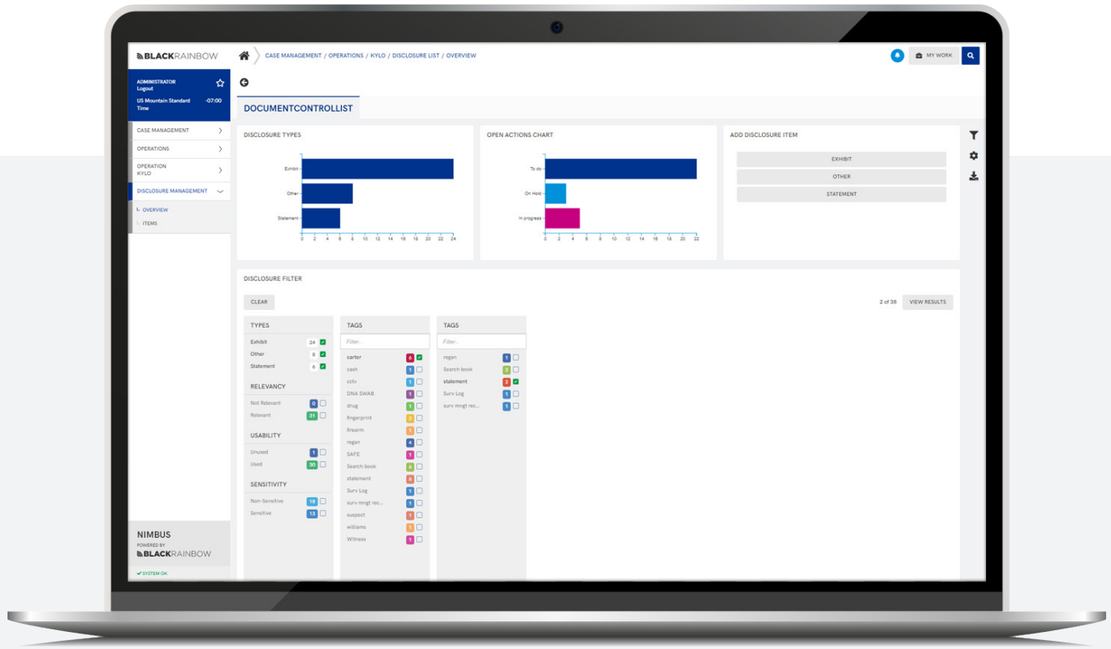
03.

Recommendation 6

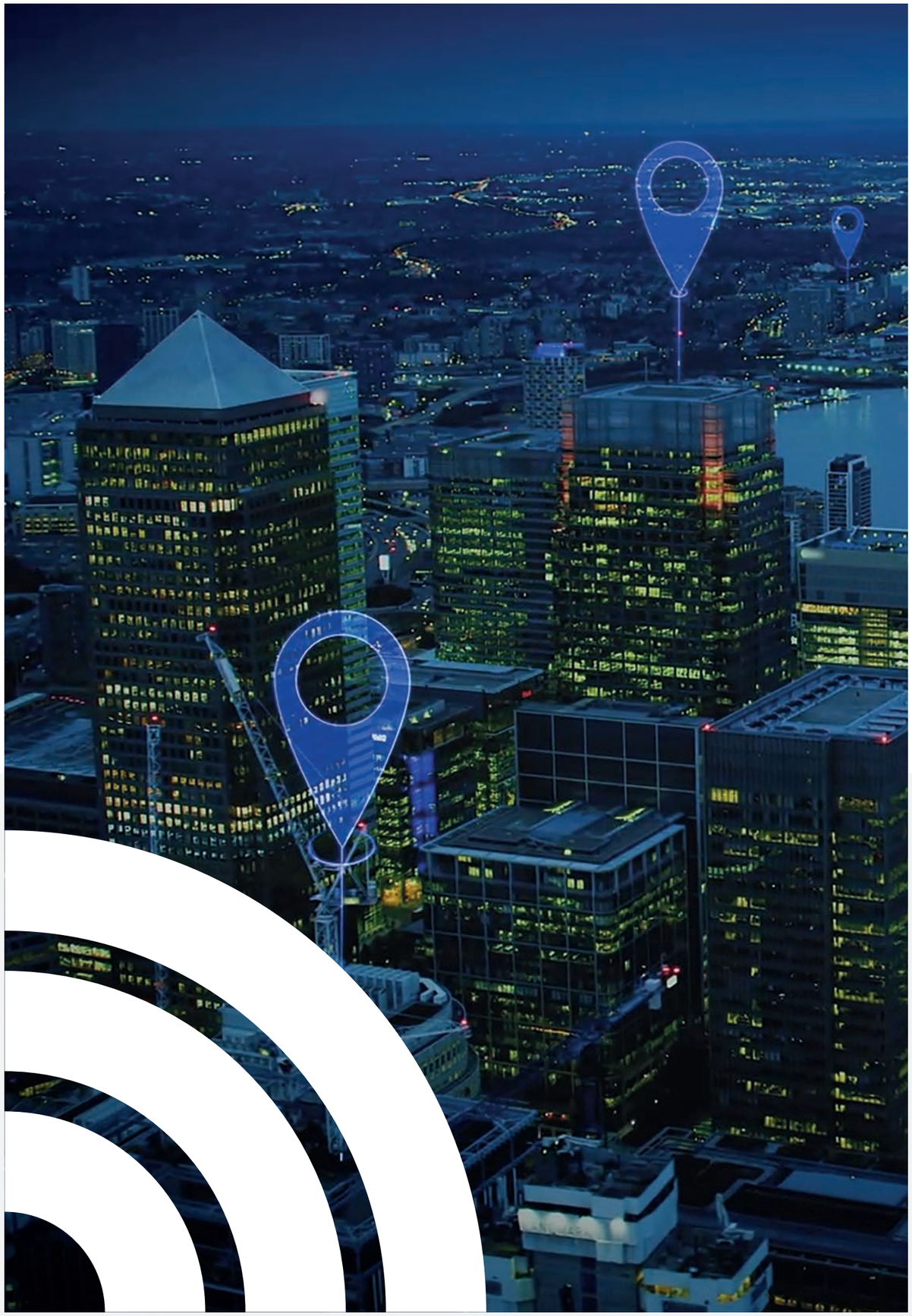
CJS early engagement

NIMBUS disclosure module allows for early engagement with the CJS by providing the categorisation of various types of disclosure material, at the data entry point and when its status/significance to the case the changes. This comprehensive disclosure functionality enables stakeholders, such as the CPS, to access the disclosure module and communicate requirements.





BLACKRAINBOW



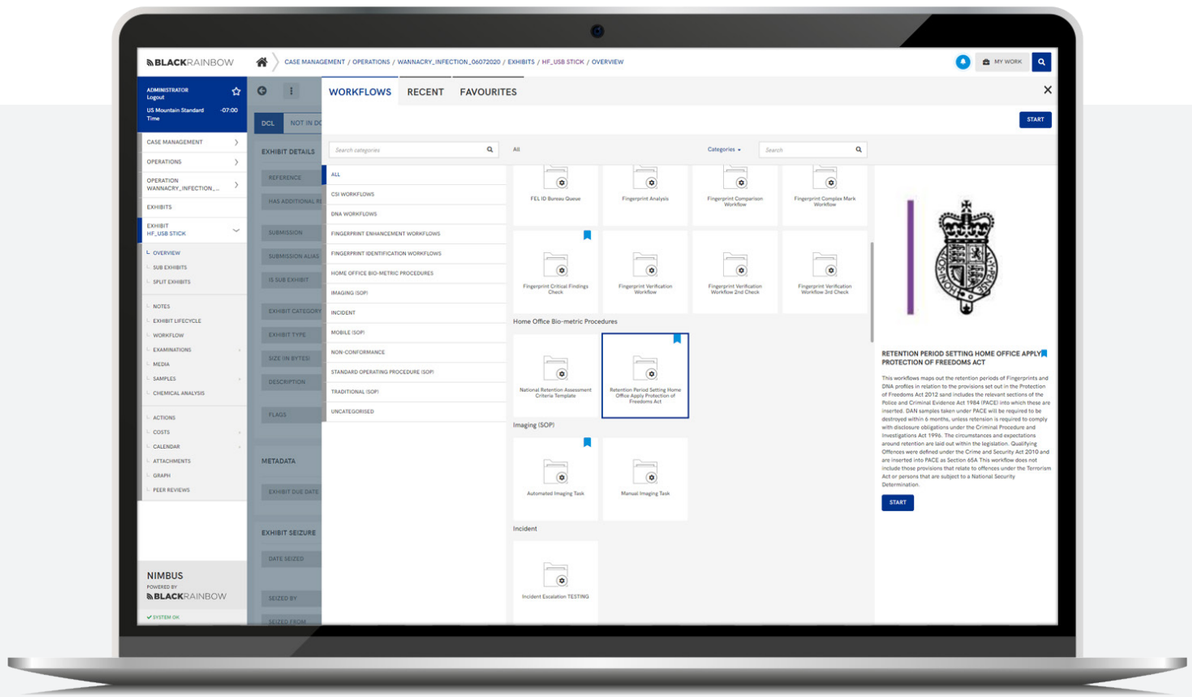
04.

Recommendation 7

Retention

NIMBUS manages the compliance, disclosure and retention of personal data by linking, automating and controlling forensic extractions, including any subsequent search and analytics. The central management of data within NIMBUS ensures only the data authorised or consented is extracted and is handled in accordance with all relevant legislation.

NIMBUS is able to control all assets and the data stored within, ensuring data is stored securely and identifiable for the application of retention requirements under any relevant legislation such as DPA 2018 and CPIA 1996.



BLACKRAINBOW

05.

Recommendation 8

Enhanced engagement with phone owners

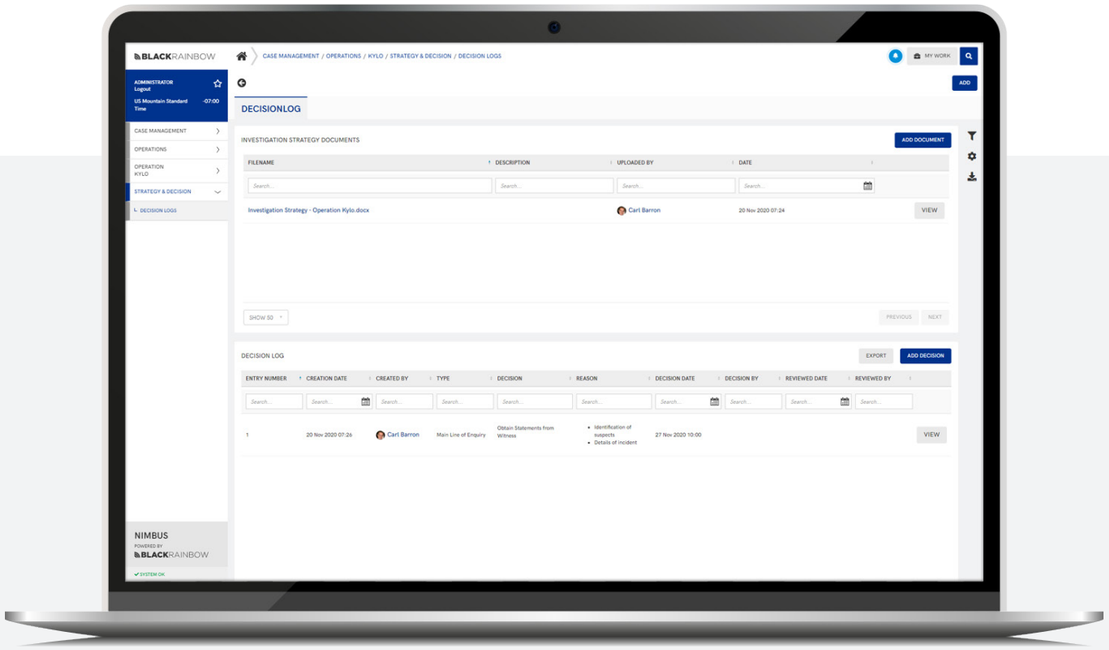
NIMBUS ensures that only the required data is extracted by managing digital forensic strategies and any subsequent automation of 3rd party software. If the strategy is revised, NIMBUS workflow management notifies officers, advising the grounds for the change and the level of privacy information that needs to be shared with the phone owner.

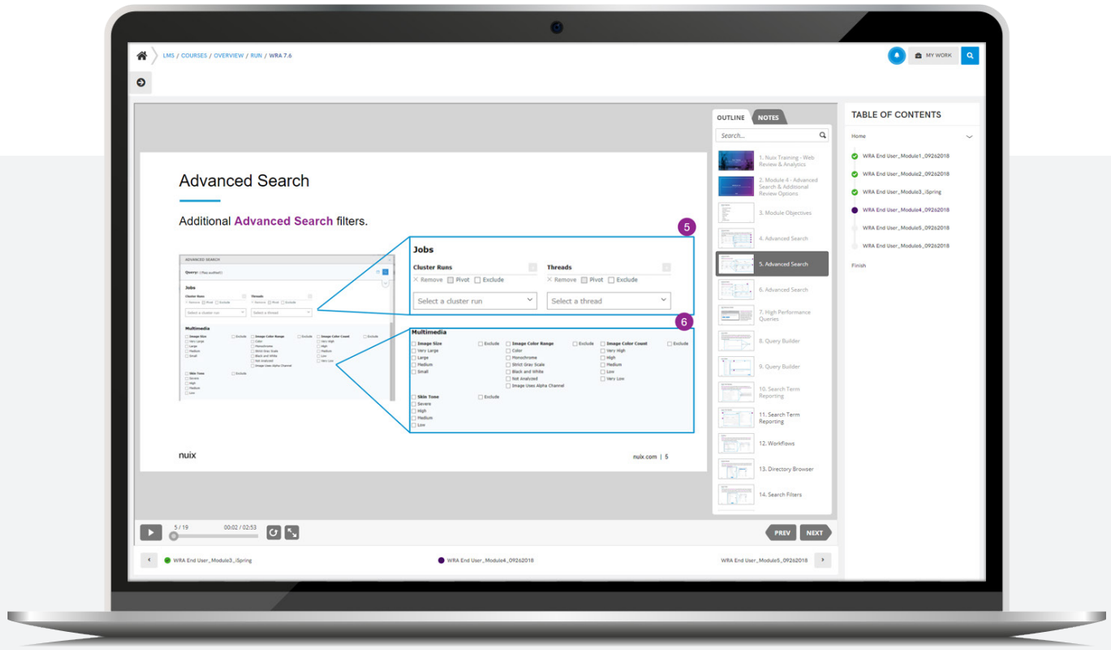
06.

Recommendation 9

National Training Standard

NIMBUS is able to deliver national training standards through its integrated learning management system (LMS). The LMS facilitates both imported and home developed courses, including competency-based knowledge checks, ensuring all practitioners and decision makers are fully trained in all aspects of mobile phone extraction activity and associated data protection law.



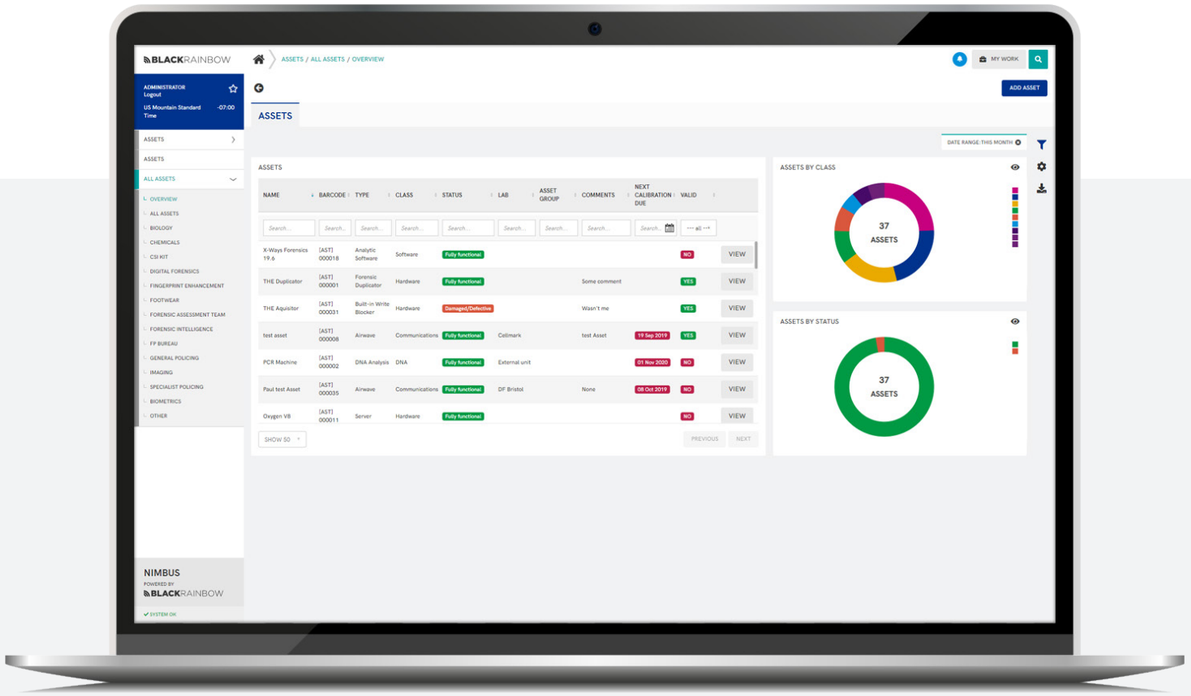


07.

Recommendation 10, 11 & 12

Technology management, DPO & DPIA

NIMBUS has been created as a transparent privacy by design product, keeping track of assets within its comprehensive asset management module, including the recording and storage of all relevant information, DPIA's, accreditations, etc. BlackRainbow's DPO can engage directly with your DPO to ensure full consultation prior to the implementation of NIMBUS.



BLACKRAINBOW

We are making great progress...

BlackRainbow recognises the part that technology can play in protecting individual human rights, whilst conducting reasonable lines of inquiry, seeking justice and protection of the public. We acknowledge and advocate technology as an 'enabler' for the transparent management of data and believe it is vital in retaining public trust and consent.

We therefore understand the immense task of successfully implementing the recommendations within the ICO report, whilst carrying out an ever-increasing workload. Nimbus is our solution to this problem and is designed to safeguard both the individual users, organisations and the wider public.

We will be detailing the areas of NIMBUS highlighted in this article over the next few weeks, so please feel free to reach out to us if you would like to know more.

THE AUTHOR

Sarah Allen
Head of Organisational Development

Sarah is responsible for the alignment, integration and development of BlackRainbow's governance, risk and compliance capabilities. Sarah also builds and implements BlackRainbow solutions, blending 17 years of operational forensic science experience, with her expert knowledge of quality management systems.

BLACKRAINBOW

Request a demo or just after more information?

T: +44(0)20 8050 9356

E: info@blackrainbow.com