BLACKRAINBOW

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

NIMBUS

COMPLEX OPERATIONS PLATFORM

CUSTOMISABLE CASE DASHBOARD REPORTING
CASE ANALYTICS & CASE DISCLOSURE
DETAILED & CUSTOMISABLE WORKFLOW BUILDING
CASE NOTES & STATEMENT / REPORT CONSTRUCTION
AUTOMATION , ORCHESTRATION & FORENSIC TOOL INTEGRATION
QUALITY MANAGEMENT & MOBILE CAPABILITY

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.

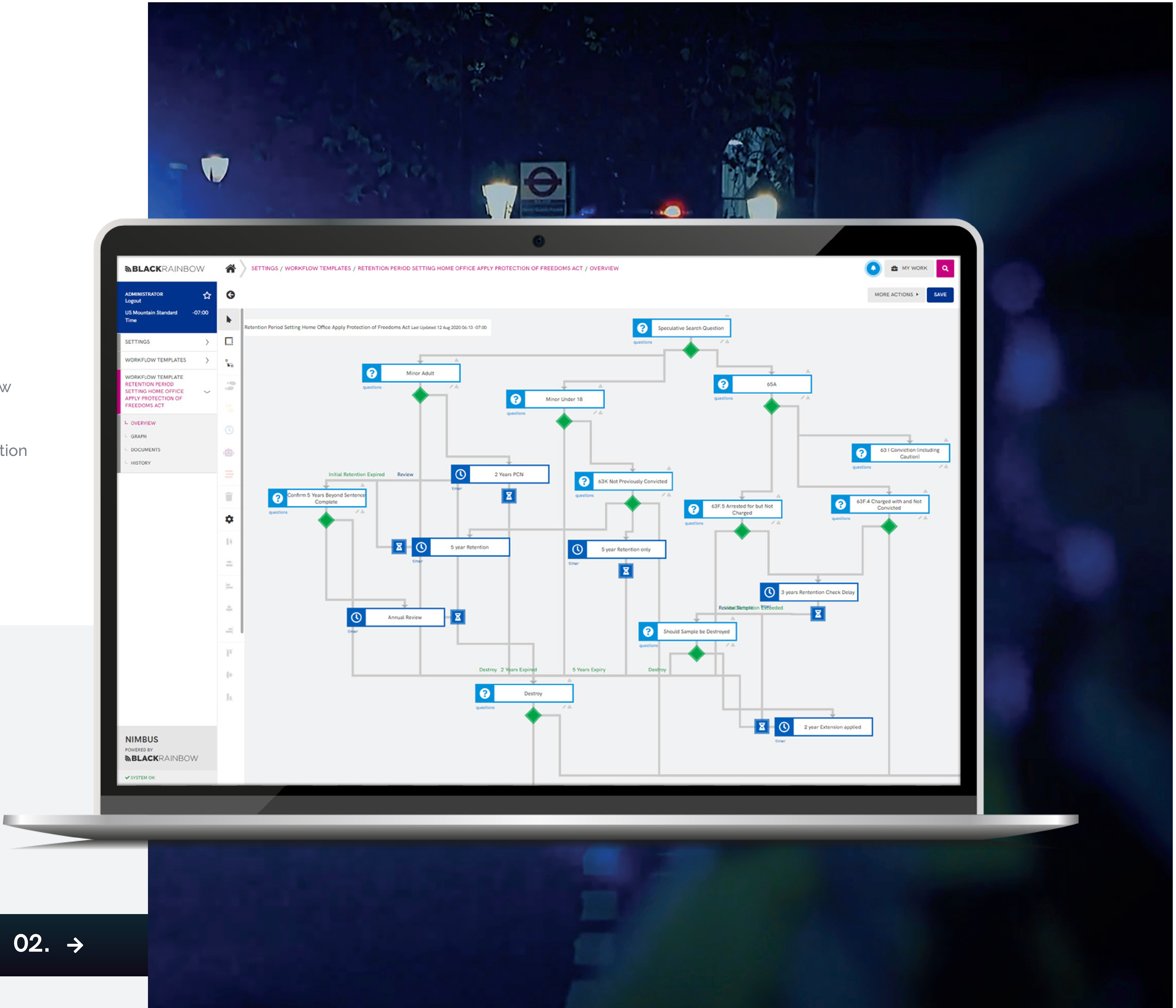
Read 7 ways NIMBUS addresses the ICO recommendations →

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.


BLACKRAINBOW
SETTINGS / WORKFLOW TEMPLATES / RETENTION PERIOD SETTING HOME OFFICE APPLY PROTECTION OF FREEDOMS ACT / OVERVIEW
MY WORK
MORE ACTIONS
SAVE
ADMINISTRATOR
Logout
US Mountain Standard Time
-07:00
SETTINGS
WORKFLOW TEMPLATES
WORKFLOW TEMPLATE
RETENTION PERIOD SETTING HOME OFFICE APPLY PROTECTION OF FREEDOMS ACT
OVERVIEW
GRAPH
DOCUMENTS
HISTORY
NIMBUS
POWERED BY
BLACKRAINBOW
SYSTEM OK

Retention Period Setting Home Office Apply Protection of Freedoms Act Last Updated: 12 Aug 2020 06:13 -07:00

Speculative Search Question
questions
Minor Adult
questions
Minor Under 18
questions
65A
questions
63 I Conviction (including Caution)
questions
Initial Retention Expired
Review
2 Years PCN
timer
63K Not Previously Convicted
questions
Confirm 5 Years Beyond Sentence Complete
questions
63F.5 Arrested for but Not Charged
questions
63F.4 Charged with and Not Convicted
questions
5 year Retention
timer
5 year Retention only
timer
3 years Rentention Check Delay
Review Sample Retention Exceeded
Annual Review
timer
Should Sample be Destroyed
questions
Destroy
2 Years Expired
5 Years Expiry
Destroy
Destroy
questions
2 year Extension applied
timer

02. →

BLACKRAINBOW

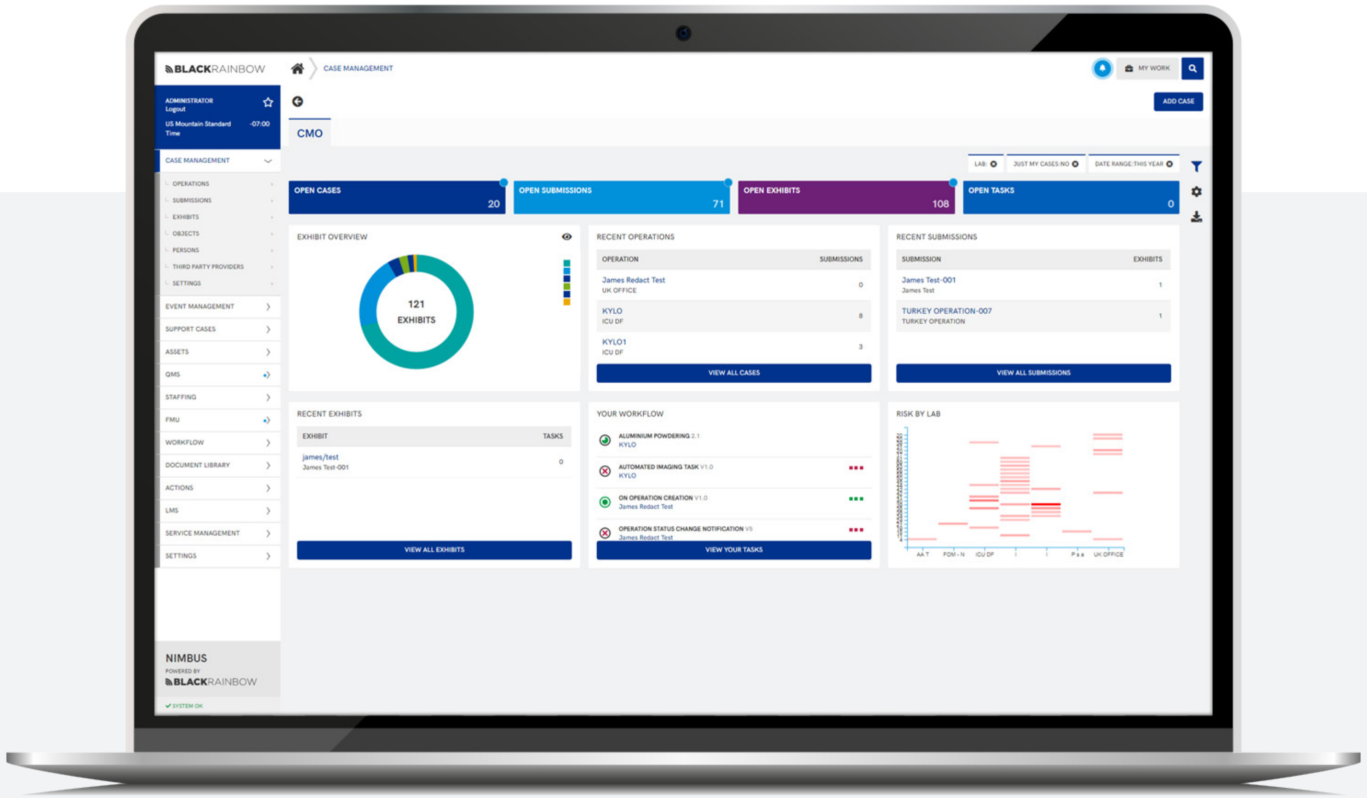
04. →

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.

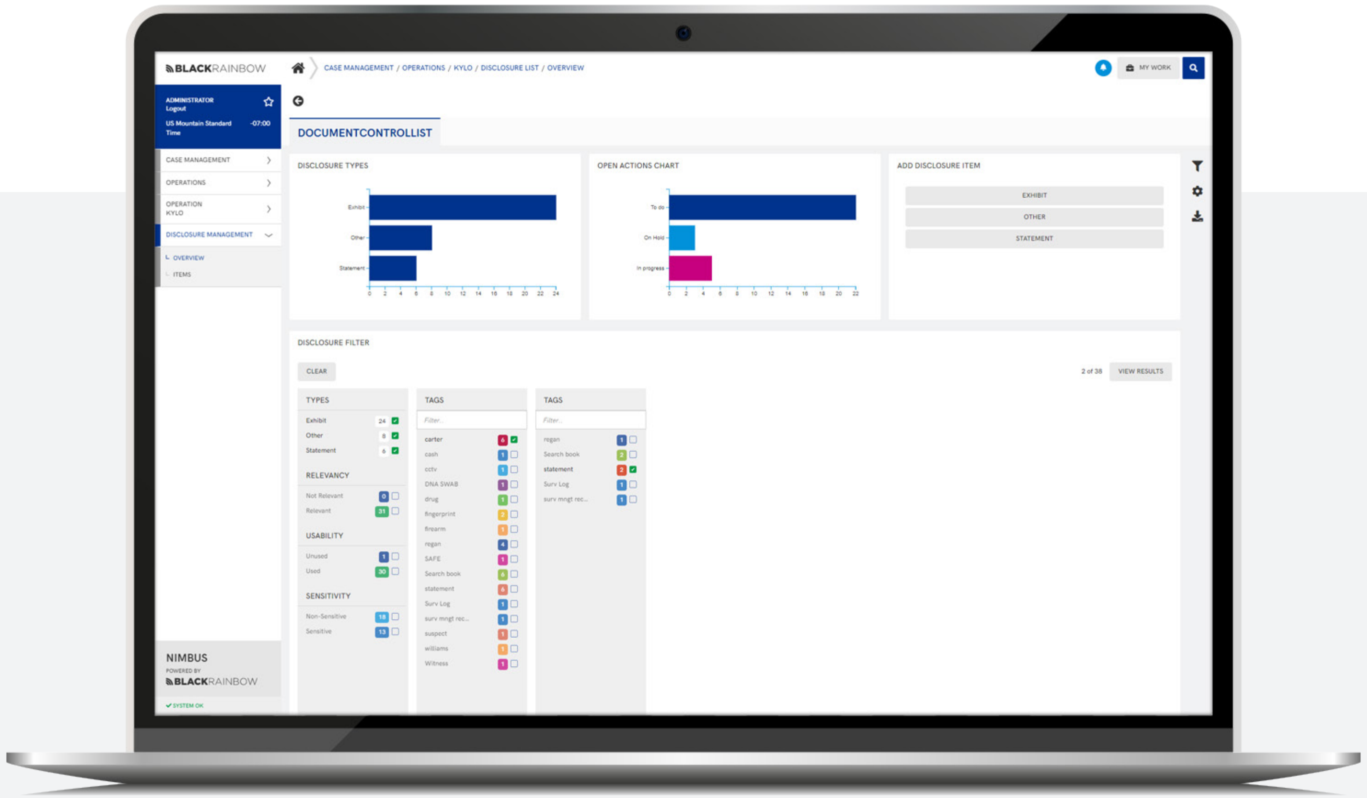


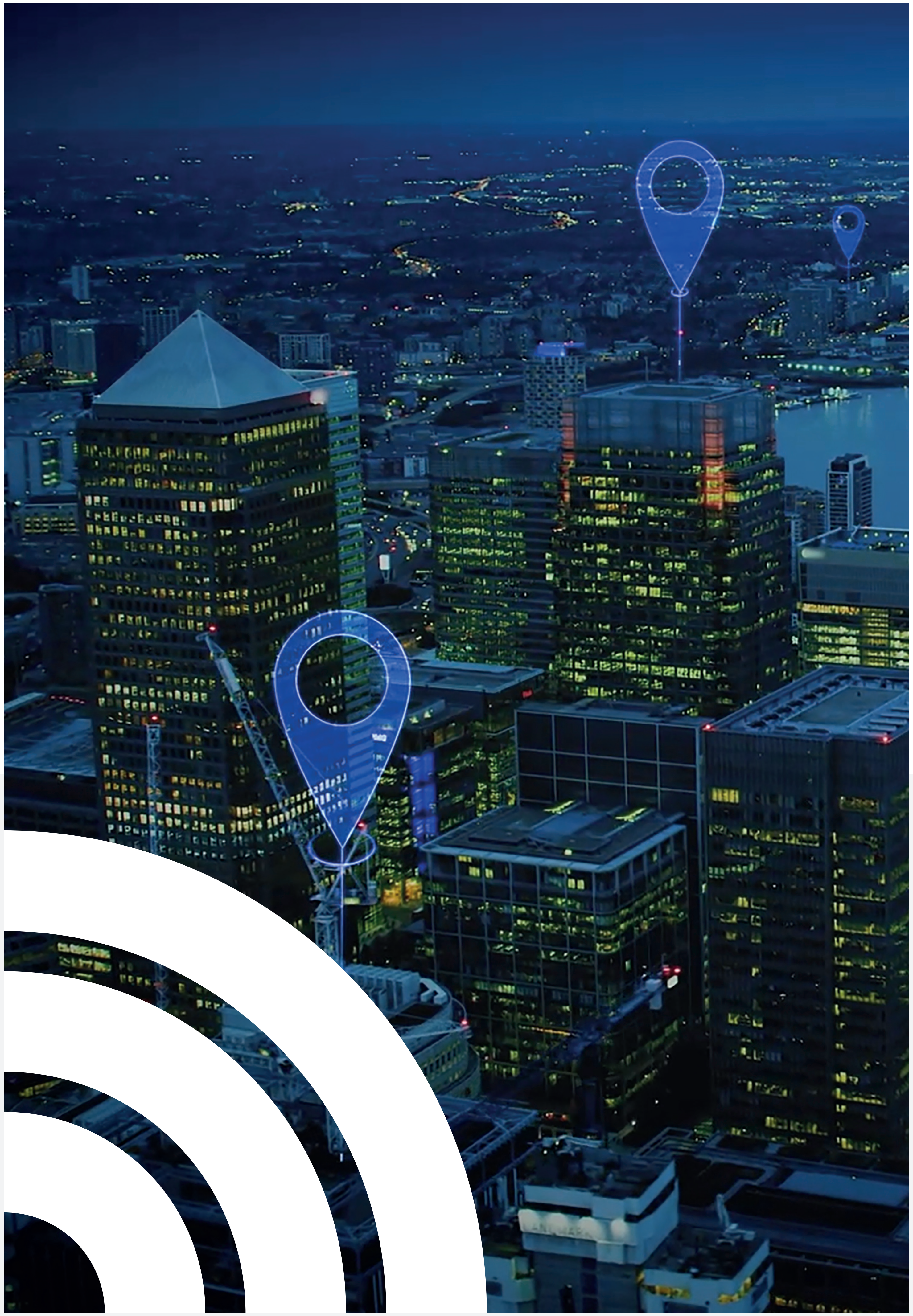
03.

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.





04.

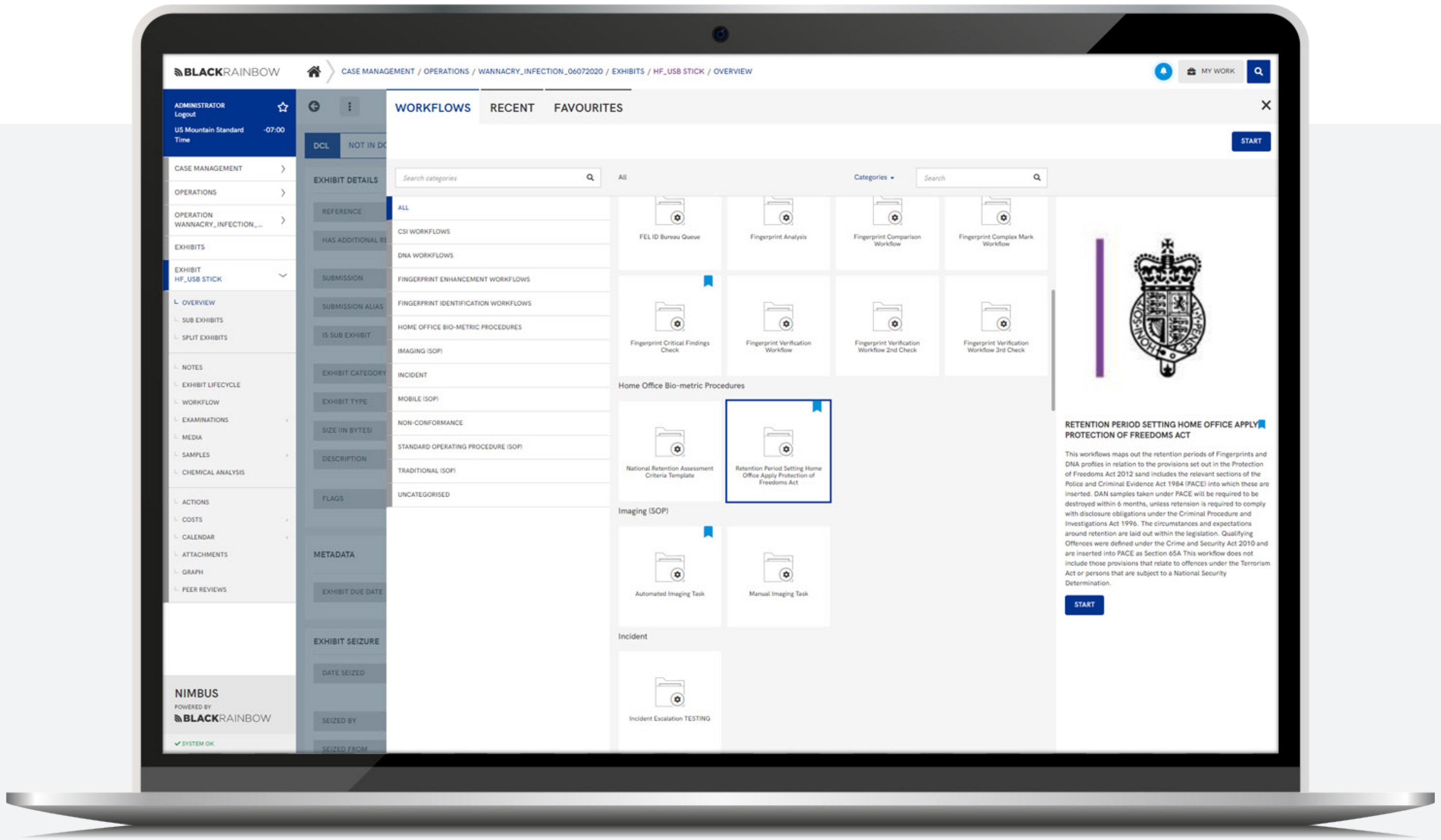
Recommendation 7

Retention

05. →

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.



This workflows maps out the retention periods of Fingerprints and DNA profiles in relation to the provisions set out in the Protection of Freedoms Act 2012 sand includes the relevant sections of the Police and Criminal Evidence Act 1984 (PACE) into which these are inserted. DAN samples taken under PACE will be required to be destroyed within 6 months, unless retension is required to comply with disclosure obligations under the Criminal Procedure and Investigations Act 1996. The circumstances and expectations around retention are laid out within the legislation. Qualifying Offences were defined under the Crime and Security Act 2010 and are inserted into PACE as Section 65A This workflow does not include those provisions that relate to offences under the Terrorism Act or persons that are subject to a National Security Determination.

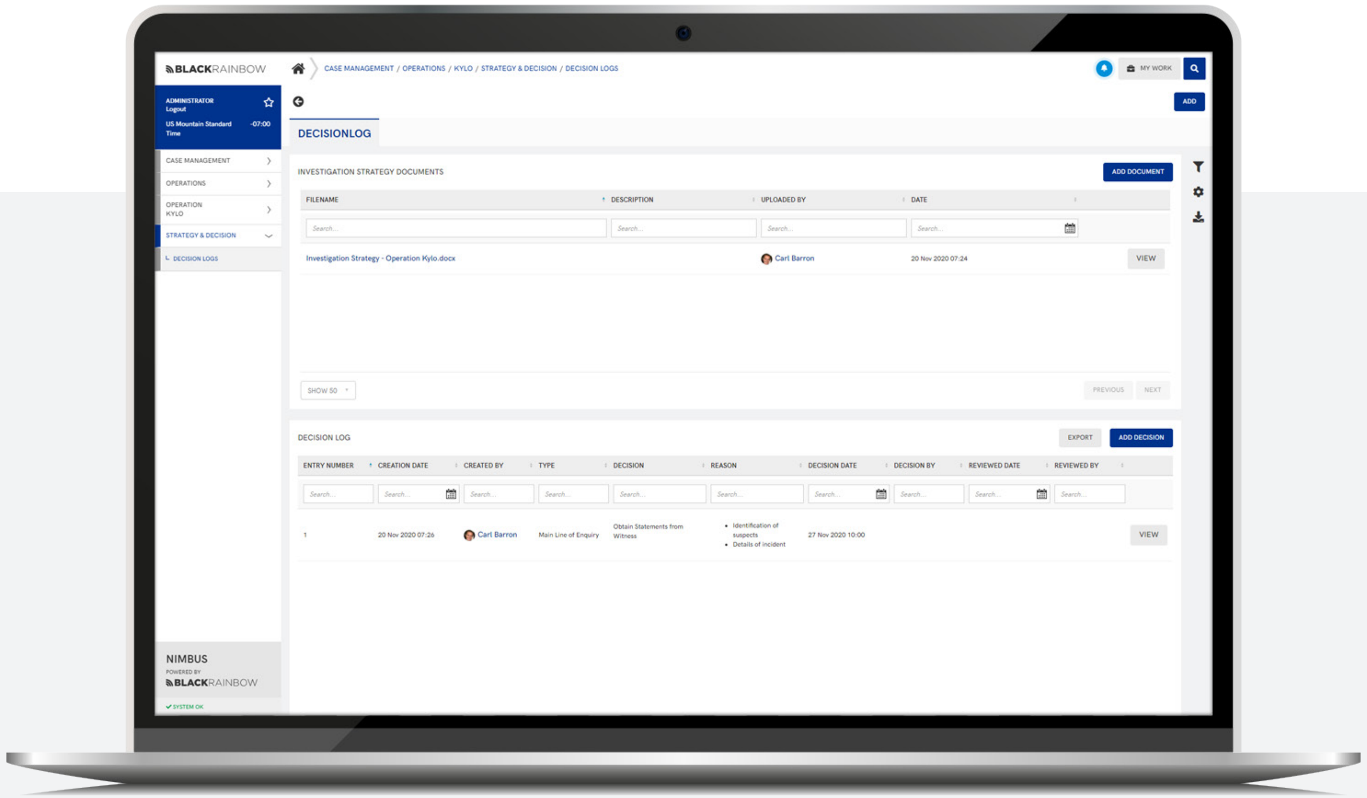
07. →

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.



INVESTIGATION STRATEGY DOCUMENTS

FILENAME	DESCRIPTION	UPLOADED BY	DATE
Investigation Strategy - Operation Kylo.docx		Carl Barron	20 Nov 2020 07:24

DECISION LOG

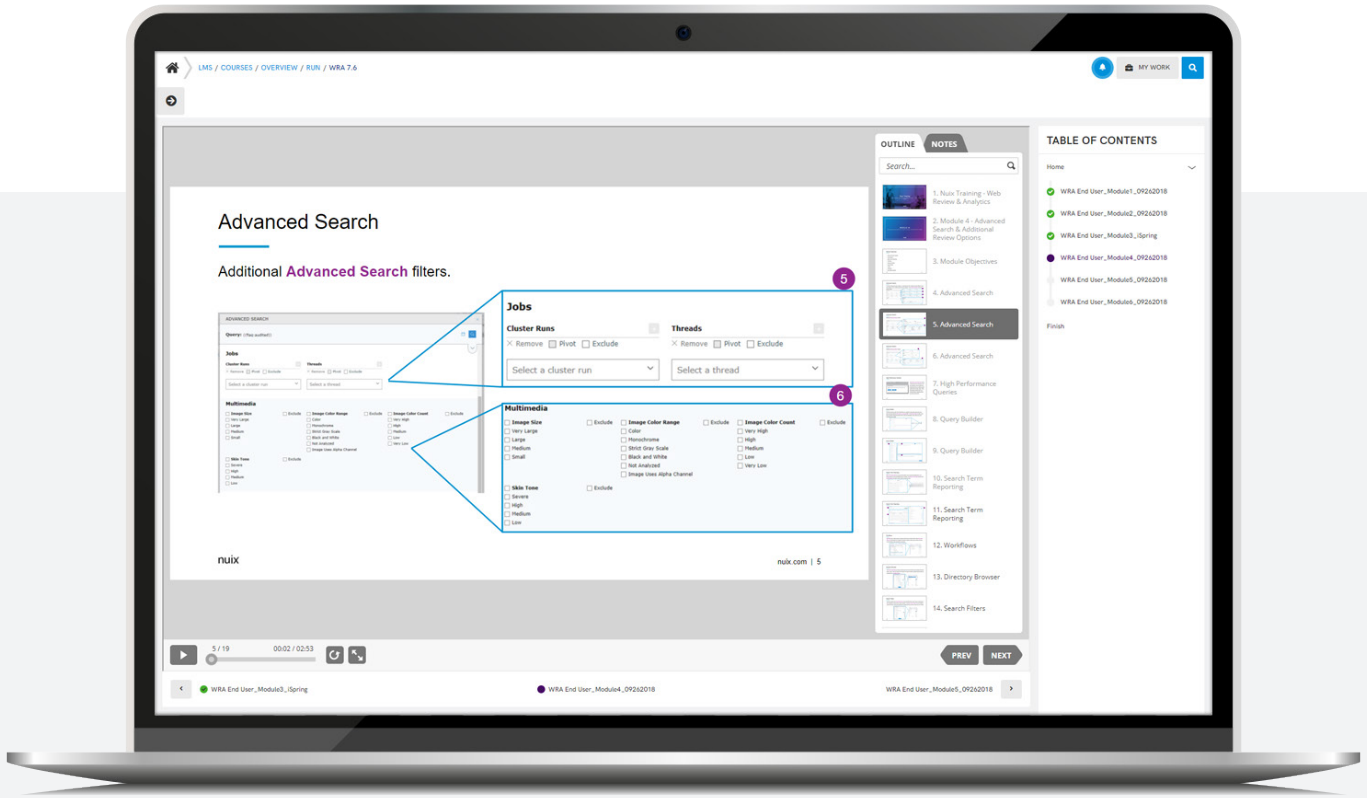
ENTRY NUMBER	CREATION DATE	CREATED BY	TYPE	DECISION	REASON	DECISION DATE	DECISION BY	REVIEWED DATE	REVIEWED BY
1	20 Nov 2020 07:26	Carl Barron	Main Line of Enquiry	Obtain Statements from Witness	• Identification of suspects • Details of incident	27 Nov 2020 10:00			

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.

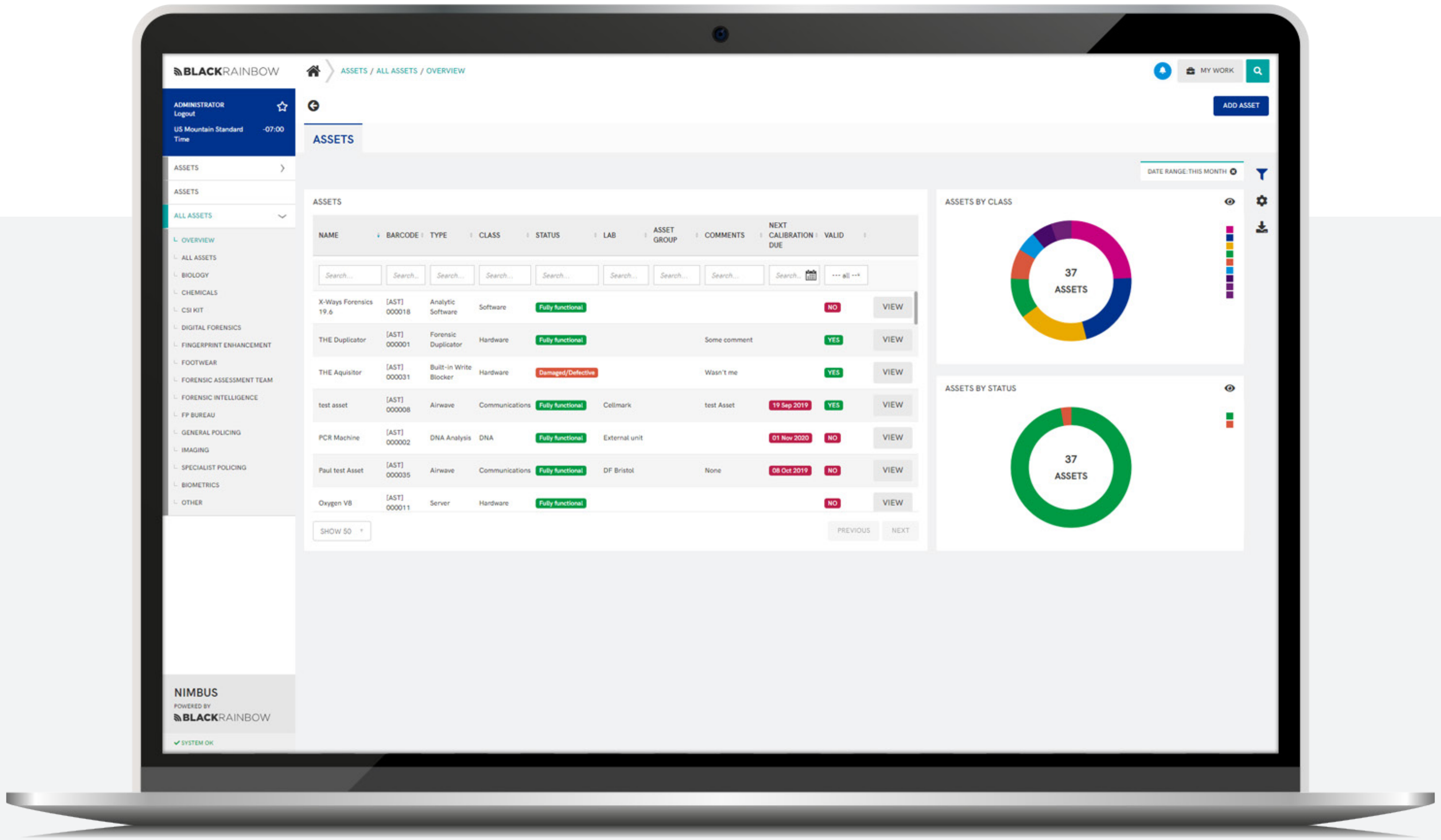


07.

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.



ASSETS

NAME	BARCODE	TYPE	CLASS	STATUS	LAB	ASSET GROUP	COMMENTS	NEXT CALIBRATION DUE	VALID	
Search...	Search...	Search...	Search...	Search...	Search...	Search...	Search...	Search...	--- all ---	
X-Ways Forensics 19.6	[AST] 000018	Analytic Software	Software	Fully functional					NO	VIEW
THE Duplicator	[AST] 000001	Forensic Duplicator	Hardware	Fully functional			Some comment		YES	VIEW
THE Aquisitor	[AST] 000031	Built-in Write Blocker	Hardware	Damaged/Defective			Wasn't me		YES	VIEW
test asset	[AST] 000008	Airwave	Communications	Fully functional	Cellmark		test Asset	19 Sep 2019	YES	VIEW
PCR Machine	[AST] 000002	DNA Analysis	DNA	Fully functional	External unit			01 Nov 2020	NO	VIEW
Paul test Asset	[AST] 000035	Airwave	Communications	Fully functional	DF Bristol		None	08 Oct 2019	NO	VIEW
Oxygen V8	[AST] 000011	Server	Hardware	Fully functional					NO	VIEW

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

www.blackrainbow.com