JDPA
JERSEY DATA PROTECTION AUTHORITY

JDPA STRATEGIC PRIORITIES

2026 - 2028

OUR VISION AND VALUES

The vision of the Authority is to create an Island culture of 'privacy by instinct'. The Authority aims to achieve this by engaging with the Island community to embrace a collaborative and innovative approach to data protection whilst providing a leading-edge model to other, similar jurisdictions.

Our values are a fundamental part of our identity, reflecting our culture. We created them to serve as constant reminders of our guiding principles, ensuring we uphold each one.

'Privacy by instinct' involves a culture where individuals and organisations naturally consider and respect privacy. This natural reflex guides our actions and choices in everyday situations, making privacy a core part of our immediate decision-making process rather than an afterthought when it's explicitly required. The attainment of our vision embodies enforcement, outreach and innovation. For example, as we would approach caution when carefully crossing the road or putting your seatbelt on before you drive. You do both to keep yourself safe, yet you most likely do not think about it as it has become instinctive over time.

To realise our vision, we need to leverage all our strengths and resources. This includes taking robust enforcement measures, conducting a broad range of outreach interventions, and leading the conversation on the importance of innovation in data protection and privacy.

This vision is essential to maintaining Jersey's position as a well-regulated, safe place to do business and is of fundamental importance to Jersey's economy, recognising that alongside its traditional agricultural and tourism industries, Jersey is also a globally recognised international finance centre.

The Authority strives to promote the data protection rights of individuals, be they our local citizens or international stakeholders, through a practical and ethical approach to business practice and regulation that supports the delivery of public services and promotes the social and economic interests of the Island.

2026–2028 STRATEGIC PRIORITIES

Introduction

Our 2026-2028 Strategic Priorities align with our vision and build on the previously embedded strategic outcomes and incorporates our new priorities alongside a transformational approach to delivery.

Our priorities coupled with our statutory mandate serve as our compass and enhances on our progress, recalibrating our approach to greater transparency, maintaining quality and stability, but most critically focusing on areas which are challenging our business community and islanders alike.

The JOIC needs to be a fit for purpose regulator, proportional and provide value for money. By embracing progressive issues, helping our community to be prepared and harnessing the benefits of technology we are centering the three priority areas which are relevant, timely and essential.

This Strategic plan will enable JOIC to successfully reset the themes along with the programmes and services to deliver our strategic priorities from 2026 onwards, considering the fast-paced and technological environment, in which we regulate.

Priority Themes

Our revised strategic focus covers three broad priorities, whilst still serving the high-level Jersey population outcomes and JOIC's purpose to 'provide those who interact with Jersey organisations and Government with the highest standard of personal data protection'. These priorities are considered core areas of concern in terms of privacy and risks to individuals.

- **ARTIFICIAL INTELLIGENCE**
  Promoting responsible local use, development and deployment of AI-driven technologies by setting out clear standards in terms of our expectation of compliance with data protection laws and principles, thereby safeguarding individuals' rights, fostering innovation, and establishing a trusted framework for ethical AI use.
- **CYBER SECURITY**
  Helping to strengthen organisations' personal data security and cybersecurity protections through clear guidance to reduce the risk of data breaches, enhance resilience against cyber threats, and ensure the ongoing privacy and safety of individuals' personal data.
- **CHILDREN'S PRIVACY**
  Helping to foster a safer digital environment to protect children's personal data by setting clear standards for organisations, promoting responsible design of digital services, and taking strong enforcement action where risks to children are identified.

Approach to Delivering our Strategic Priorities

Whilst the three priority areas are unsurprising in the current context, it is the approach to their delivery which is transformational. We will be taking a three-phased approach of Advise, Assess and Act. Our new Strategic Priorities begin from 2026 onwards, within the triple 'A' approach.

ADVISE is the phase where we support individuals and organisations to improve their data protection practices by providing information, guidance, and rights support.

ASSESS being the phase which focuses on gathering intelligence and evaluating how well data is being protected. Its purpose is to build an evidence base, identify high-risk practices, and understand where intervention is most needed.

ACT is the final phase where we will initiate regulatory action where necessary to address breaches and enforce the law. This phase addresses non-compliance and drives accountability. Its purpose is to deter misconduct, protect the public from harm and reinforce that standards are mandatory not optional.

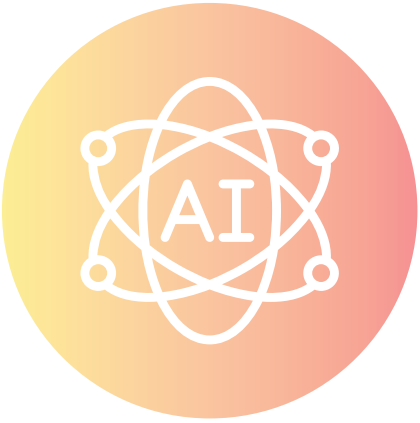
Throughout the **AAA** approach the JOIC will be monitoring any gaps in organisational capability and defining what any gap may be, and how we manage the gap, additional resources required etc.

The Authority and the JOIC leadership team have aligned our Strategic Priorities with the Island's overarching goals whilst enabling us to deal with the demands of international technological advancements, young people's online safety, complex business and individual needs, international cooperation, and enforcement. Our Strategic Priorities are vital for the sustainable development of Jersey's digital economy, and therefore for our Island's continued prosperity.

Although we are headlining the three priorities, the Authority remains as committed as ever to tackling any matter either proactively or reactively if required. We may become aware of an issue through breach reporting, data protection complaints and horizon scanning. If there is risk of harm to an individual(s) we will take the relevant enforcement measures.

PRIORITY 1: ARTIFICIAL INTELLIGENCE

Promoting responsible local use, development and deployment of AI-driven technologies by setting out clear standards in terms of our expectation of compliance with data protection laws and principles, thereby safeguarding individuals' rights, fostering innovation, and establishing a trusted framework for ethical AI use.



The use of AI systems in Human Resources

Automated processing systems have been used in Human Resources for decades to assist with recruitment selection and shortlisting. However, the advent and availability of AI technologies have transformed HR processes, with AI tools being used for recruitment, performance and absence management, learning and development and employee engagement analysis.

Using such tools to make decisions about employees comes with inherent privacy risks, for example, the misuse of personal information, excessive surveillance, data security issues and insufficient transparency around data processing.

The AAA Approach for Artificial Intelligence

ADVISE

Define expectations, build capability and enable compliance.

Purpose: To provide clarity regarding the responsible adoption and use of AI in HR and to prevent breaches by improving knowledge, building organisational capability and shaping good practice.

ASSESS

Evaluate compliance, performance, and risk against regulatory expectations.

Purpose: Establish an evidence base to understand what AI is and how it is being applied in the field of HR. Identify systemic trends, gaps in capability or compliance, risk profiles and priorities to inform policy and targeted advisory guidance and support.

ACT

Take targeted action to address non-compliance and uphold data protection standards.

Purpose: Ensure accountability through investigation and enforcement, correcting non-compliance, deterring unsafe practices, and protecting personal data.

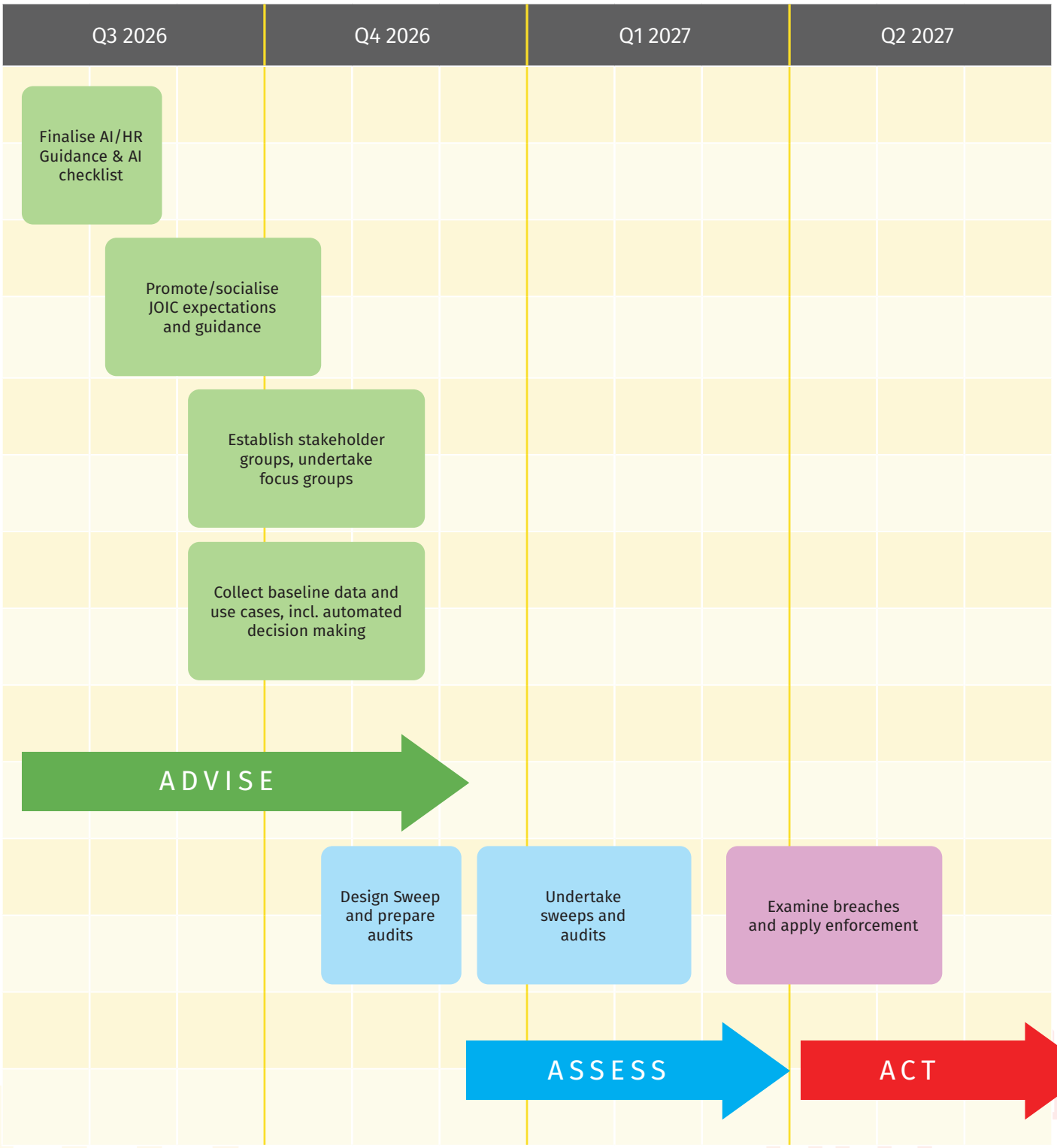
Headline Indicators

This programme includes a mix of operational delivery indicators, emerging outcome-based measures, and contextual intelligence metrics. In recognition of the early-stage nature of this regulatory priority, the initial focus will be on establishing robust baseline data across key indicators and building a clear understanding of AI use in HR processes.

Where sufficient data maturity exists, proportionate targets have been set; where not, measures will be used to establish baselines and inform future target setting and benchmarking. Contextual intelligence measures are included to support regulatory insight and do not require targets.

HEADLINE AREA	PERFORMANCE MEASURE
Stakeholder Engagement	% of engagement sessions resulting in improved participant understanding (based on post-session evaluation)
Guidance Uptake	% of registered entities identified as using AI-in-HR processes that report application of AI-in-HR guidance
Monitoring Activity	% of audits identifying areas for improvement in AI-in-HR governance and controls
Investigation Timeliness	% of priority AI-in-HR cases assessed and progressed within agreed internal timeframes
Enforcement Effectiveness	% of enforcement actions resulting in sustained compliance

AI-in-HR Strategic Priority Timeframe



PRIORITY 2: CYBER SECURITY

Helping to strengthen organisations' personal data security and cybersecurity protections through clear guidance to reduce the risk of data breaches, enhance resilience against cyber threats, and ensure the ongoing privacy and safety of individuals' personal data.

Data security is central to compliance with any data protection regime, and the Data Protection (Jersey) Law 2018 is clear on the requirements of controllers and processors, including when and how they should log and report data breaches. The value in reporting breaches comes from the lessons learned, and in a world where cybercrime is becoming more prevalent, data security frameworks should, by default, include measures to protect against cyber threats.

Our data shows that unauthorised access and unauthorised disclosure are the two main underlying causes of data breaches in Jersey. As the regulator we need to have a greater understanding and awareness of the causes along with the controls and measures being deployed to prevent them, and the frequency of review.

The AAA Approach for Cyber Security

ADVISE

Define expectations, build capability and enable compliance.

Purpose: To provide clarity regarding breach prevention by, improving knowledge, building organisational capability and shaping good practice.

ASSESS

Evaluate compliance, performance, and risk against regulatory expectations.

Purpose: Establish an evidence base to understand the causes along with the controls and measures being deployed to prevent the two main causes of data breaches in Jersey. Identify systemic trends, gaps in capability or compliance, risk profiles and priorities to inform policy and targeted advisory guidance and support.

ACT

Take targeted action to address non-compliance and uphold data protection standards.

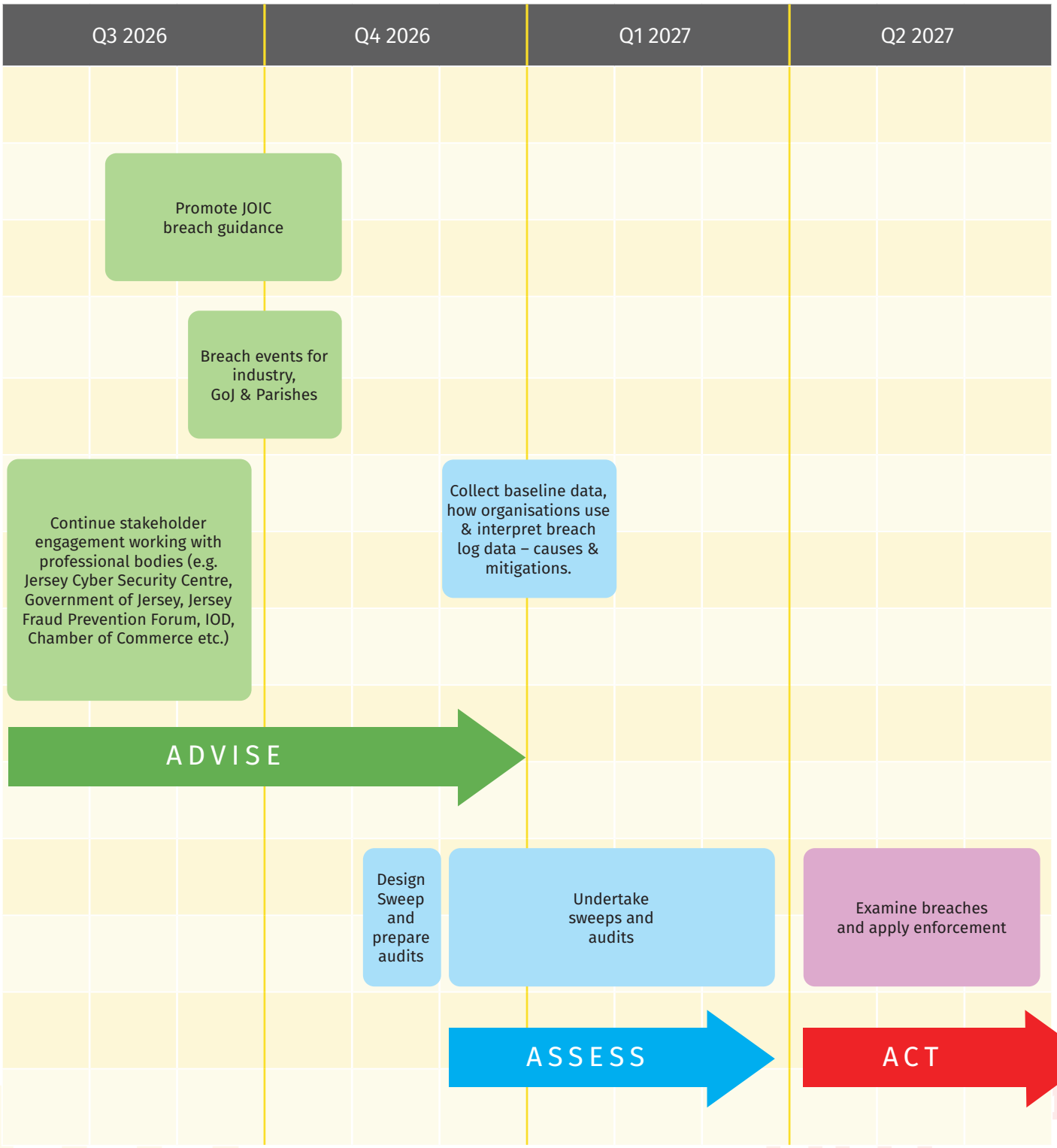
Purpose: Ensure accountability through investigation and enforcement, correcting non-compliance, deterring unsafe practices, and protecting personal data.

Headline Indicators

In recognition that cyber security is a more established regulatory area with increasing data maturity, the focus has shifted from initial baseline establishment towards a mix of operational delivery measures and emerging outcome-based indicators. While a more robust evidence base is now available, movements in indicators (whether upward or downward) must be interpreted with caution and in context, to ensure changes in reporting, awareness, and enforcement activity are properly understood. Where appropriate, proportionate targets will be considered; however, continued refinement of trend analysis will inform future performance expectations and interpretation.

HEADLINE AREA	PERFORMANCE MEASURE
Stakeholder Engagement	% of organisations reporting increased understanding of cyber security risks and mitigations following engagement % of organisations rating regulatory engagement as useful in strengthening their cyber security practices
Guidance Uptake	% of organisations reporting they have implemented or updated controls based on regulatory guidance
Monitoring Activity	% of audits identifying areas for improvement in cyber security governance and controls
Investigation Timeliness	% of audits identifying areas for improvement in cyber security governance and controls audits
Enforcement Effectiveness	% of incidents arising from organisations with prior similar breaches
Priority Outcomes	Rate of unauthorised access and unauthorised disclosure incidents per 100 registered entities % of incidents reported within required timeframe

Cyber Security Strategic Priority Timeframe



PRIORITY 3: CHILDREN'S PRIVACY

This Priority focuses on Children's Privacy in the context of education technology and the use of online platforms and services. It aims to help foster a safer digital environment to protect children's personal data by setting clear standards for organisations, promoting responsible design of digital services, and taking strong enforcement action where risks to children are identified.

As more educational establishments look to streamline and improve their services, educational technologies are becoming more widespread in schools, with a huge number of platforms on offer to assist with teaching, personalised learning, coordination of lesson schedules and more. The tools on offer include innovative solutions such as AI tutors, assistive technologies (particularly young people with learning difficulties or visual impairments), cloud-based services for collaborative working and educational apps.

EdTech is the umbrella term used to describe the use of education technologies to support and enhance teaching and learning. It includes a wide range of tools and resources and is used in a variety of settings to improve the effectiveness and efficiency of education.

From online learning platforms to adaptive learning software and virtual reality simulations, EdTech is helping to revolutionise the way we learn and grow.

Whilst clearly useful, educational and groundbreaking, many of these tools come with significant privacy risks, particularly around access and storage of personal data, but also around surveillance, and the risk of data breaches, the secondary commercial use of student information, algorithmics bias and excessive personal data collection.

Discussions around online harms remain ongoing at the time of writing. However, irrespective of the outcomes of those discussions, we will be working with other regulators and bodies such as the Children's Commissioner, the NSPCC and the Children, Young People, Education and Skills Department (CYPES), who have already undertaken research in this area to help inform our approach in Jersey.

In setting this Priority, JOIC recognises the important contribution it can make through interpreting and enforcing data protection law, issuing guidance specific to children's data, investigating breaches, and holding organisations accountable. In this developing area, it also has a key role to play in offering guidance and support to schools and EdTech providers.

The AAA Approach for Children's Privacy

ADVISE

Define expectations, build capability, and enable compliance

Purpose: To prevent breaches by providing clarity, improving knowledge, building organisational capability and shaping good practice.

ASSESS

Evaluate compliance, performance, and risk against regulatory expectations.

Purpose: Establish an evidence base to understand how well children's data is being protected in EdTech. Identify systemic trends, gaps in capability or compliance, risk profiles, and priorities to inform policy as well as targeted advice, guidance and support.

ACT

Take targeted action to address non-compliance and uphold data protection standards.

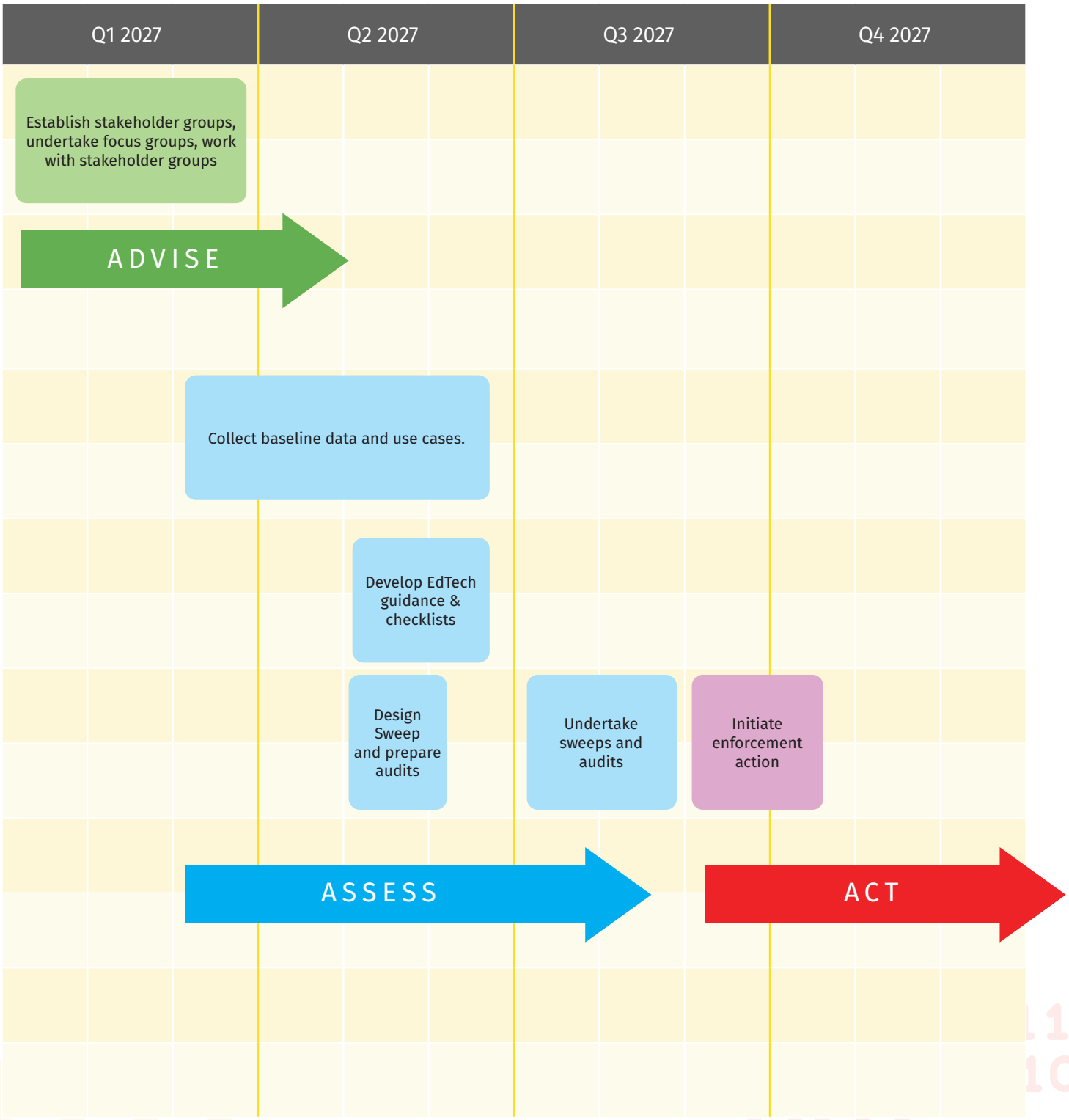
Purpose: Ensure accountability through investigation and enforcement, correcting non-compliance, deterring unsafe practices, and protecting children's data.

Headline Indicators

This program includes a mix of operational delivery indicators and emerging outcome-based measures. In recognition of the early-stage nature of this new regulatory priority, the initial focus will be on establishing robust baseline data across key indicators. Where sufficient data maturity exists, proportionate targets have been set; where not, baseline development will inform future target setting and benchmarking.

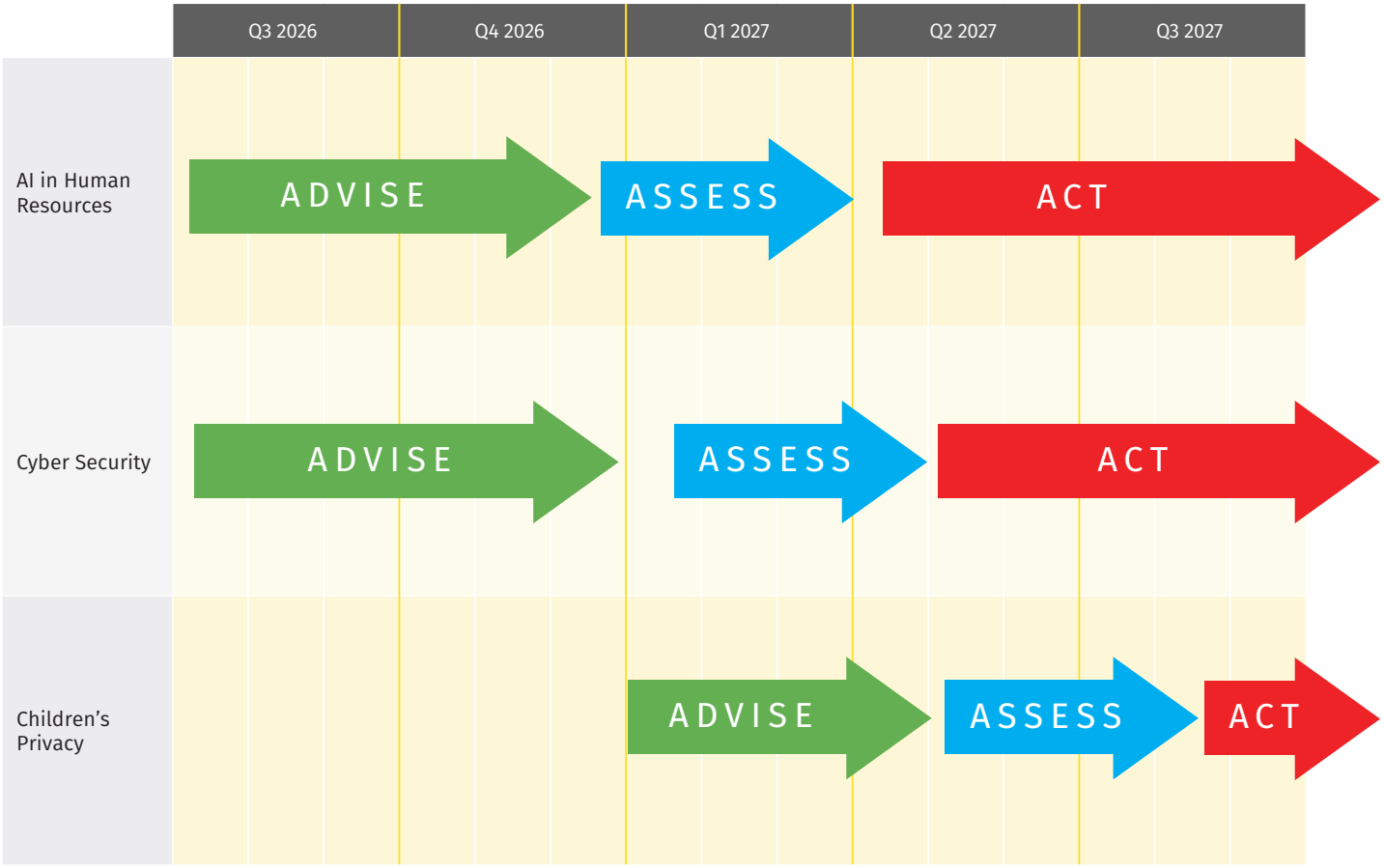
PURPOSE	PERFORMANCE MEASURE
Sector Reach	% of school/education DPOs reached through engagement activities (Year 1)
Sector Understanding	% of key education stakeholders reporting clear understanding of regulatory priorities
Monitoring Coverage	% of schools/colleges with EdTech usage mapped (Year 1)
Investigation Effectiveness	% of priority (high-risk) cases progressed or resolved within defined timeframes
Enforcement Impact	% of enforcement actions resulting in sustained compliance

Children's Privacy Strategic Priority Timeframe



SCHEDULING ADVISE, ASSESS & ACT

The image below captures the phasing of the three strategic priorities for 2026 into 2027.



MANAGING PERFORMANCE - THE PERFORMANCE AND IMPACT FRAMEWORK

We exist to enforce and help promote data protection standards in Jersey, so we need to know if change is happening and whether our programmes and services are helping to make a difference. Performance data within the Framework helps answer these questions, so we can learn and adapt as necessary.

Regulatory Service Areas

We track JOIC's effectiveness across all areas by measuring performance in three ways:

How much did we do?

We measure the **quantity** of our activities, for example how many complaints or registrations did we receive?

How well did we do it?

We assess the **quality** of our activities by measuring their effectiveness. For example feedback on awareness sessions.

Is anyone better off?

We measure the **impact** of our activities, such as improved compliance, increased understanding of data protection responsibilities, and stronger data protection practices across organisations. For example, organisations that change their practices following our advice.

By using performance information to learn, adapt and improve our services, we aim, over time, to help make a positive impact on the Island Indicators mentioned above.

MANDATED ACTIVITIES 'BUSINESS AS USUAL' MEASUREMENTS

Whilst the three priorities are integral to our transformational process, we will remain diligently engaged with business as usual (BAU) as per our mandate.

BAU includes our routine processes and day to day activities, such as communications and outreach events, dealing with enquiries and complaints and support activities to ensure our operations run smoothly.

The JOIC will continue to measure its BAU, using the same methodology, where possible, to ensure we are effective, e.g. 'how much did we do?', 'how well did we do it?' and to ensure we are having the desired impact – 'is anyone better off?'.

JOIC'S SUPPORT SERVICES

Everyone, regardless of their role, is responsible for contributing to the success of the Performance and Impact Framework. JOIC's support services including Finance, Legal, IT, Administration and Human Resources provide critical expertise, systems, processes and assistance to the wider JOIC team.

The success of the JOIC's support services is assessed not only by the quantity of activities delivered, but by the extent to which those activities enable internal teams to achieve defined outcomes and deliver impact within the Regulatory Services Areas.

JDPA
JERSEY DATA PROTECTION AUTHORITY