Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

AusCheck

Implementing a single issuing body for aviation and maritime security identification cards (ASICs and MSICs)

Discussion Paper - November 2022

Contents

Who should read this paper?

The transport sector is part of Australia's critical infrastructure, delivering essential services that are crucial to our way of life.

Transport security regulation to protect Australians, and the infrastructure we depend on, was developed over several decades. The current arrangements were established nearly 20 years ago and have been progressively strengthened and enhanced since then.

This Discussion Paper sets out a further improvement in the schemes affecting many who work in the aviation, maritime and offshore oil & gas sectors. There are real opportunities to improve how the current ASIC and MSIC schemes are managed, improving services for applicants while reducing costs for industry. The improvements explored in this paper will also create a foundation for further improvements built on the creation of a single card management system.

Impacts for individual employees and contractors will be mostly minor. But for existing issuing bodies and their staff, the changes will be fundamental, and for other employers in these sectors some changes may be significant.

We are therefore keen to hear from the following industry participants and stakeholders, given their importance to our economy, security and sovereignty:

- Regulated industry participants subject to the *Aviation Transport Security Act 2004* (the ATSA) or *Maritime Transport and Offshore Facilities Security Act 2003* (the MTOFSA)
- Issuing bodies currently appointed under the ATSA and/or the MTOFSA frameworks
- Industry organisations and employee organisations representing organisations and workers in the aviation, maritime, offshore oil & gas and air cargo sectors
- Stakeholders who depend on the aviation, maritime, offshore oil & gas and air cargo sectors and who anticipate the proposed changes may impact them, and
- Australians who embrace the need for continuous improvement to treat trusted and malicious insider risks in the ASIC and MSIC schemes; blending sector, employment, worker and national security outcomes.

Overview

What the Australian Government announced

On 25 January 2022, the Government announced that the Department of Home Affairs (the Department) would become the sole issuing body for ASICs and MSICs. It was announced that the single issuing body model will replace the current model, under which ASICs and MSICs can be issued by a range of businesses and industry stakeholders – building on critical legislation passed in June 2021 that prevents people with serious criminal backgrounds or links to serious and organised crime from accessing secure areas.

Numerous reports by Parliamentary Joint Committees, including the Committee for the Australian Commission for Law Enforcement Integrity1, identified a need for improvements in the management of ASICs and MSICs. Problems have long been identified in the protection of sovereign data relating to cardholders and issuing bodies who are responsible for the cards as well as in existing arrangements for the administration of ASICs and MSICs.

The Department is leading the implementation of this reform, which will establish a cyber-secure, effective, efficient, economical, and ethical single issuing body for the ASIC and MSIC schemes.

This change is expected to have the following benefits:

- Streamlined card processes and user authentication
- Enhanced industry confidence from nationally-consistent improvements in identifying operational need
- Improved supply chain control for cards
- Reduced regulatory burden, especially in the management of data and cyber security relating to security identification cards, and
- No ongoing requirement for employers and facility operators to invest in ICT to meet issuing body cyber security obligations.

[1] *Integrity of Australia's Border Arrangements 2020* report, Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity

Your participation

The Department is seeking stakeholder participation in consultation and planning. This Discussion Paper is one of the consultation processes to inform the Department's implementation of the single issuing body for ASICs and MSICs.

Recently, the Department conducted extensive one-on-one discussions and site visits with issuing bodies, industry participants, facility operators, trade unions and peak associations.

This Discussion Paper grew from those engagements and:

- summarises what you have told us in industry meetings, site visits and 'Town Hall' industry forums
- sets out what we have heard, and the project delivery approach we propose
- seeks your feedback on our proposed core capability model, and the Department's approach to implementation, and
- shares the approach we propose for collaboration with industry and the opportunities to optimise a long-term operating model.

Throughout this Discussion Paper, a Call for response highlights where we are seeking your views. We also welcome any other comments you may wish to make to help the Department deliver on the security objectives underpinning the reform.

Where we need to be – a single issuing body

Our vision for security identification schemes in AusCheck

Our vision is for a cyber-secure, streamlined, user focused and transparent system for security identification services which will support the best available identity verification methods appropriate to each of the schemes AusCheck administers under the *AusCheck Act 2007*.

For the ASIC and MSIC schemes, the single issuing body in AusCheck will support the needs of all users: individuals, employers and infrastructure facility operators.

AusCheck will initially focus on the transition to a single issuing body. Following this, we will be in a position to progress other service and policy reforms, further enhancing the usability and security of the schemes.

The *Transport Security Outlook to 2025* [2] identified new and evolving technical opportunities that could be implemented across transport sectors and evolving threat environments, providing opportunities to increase the identity security of our aviation and maritime industries.

Some possible enhancements to explore include front-loading the identification verification process, utilising biometric capture and anchoring capability; changes to the validity period for cards, extending them to requiring renewal only every five years and; streamlining the renewal process for existing card holders by leveraging off identity verification and biometric anchoring completed upon entry to AusCheck. Any enhancements utilising biometrics data will align with the *Privacy Act 1988* and be accompanied by the required policy, technical and security authority ensuring appropriate data and cyber security controls are in place.

Background and context

Risks to the secure and effective performance of Australia’s critical infrastructure are varied and ever present. These can emanate from inside or outside an organisation and range from hostile or criminal activity, foreign interference, terrorism, espionage and natural disasters through to poor cyber security, physical, and personnel practices. The impact of an incident can also include cascading consequences for multiple assets and services.

Across the world, cybercrime targeting essential services – such as the health care, food distribution and energy sectors – has demonstrated the vulnerability of critical infrastructure. The Australian Cyber Security Centre (ACSC) found that around one quarter of cyber security incidents reported in the 2020–21 financial year affected entities associated with Australia’s critical infrastructure3.

Similarly, the Australian Security Intelligence Organisation (ASIO) has noted that the increasingly interconnected nature of Australia’s critical infrastructure exposes vulnerabilities that, if targeted, could result in significant consequences for our economy, security and sovereignty. ASIO remains concerned about the potential for Australia’s adversaries to pre-position malicious code in critical infrastructure, particularly in areas such as telecommunications and energy.

In 2020-21, the Australian Parliament passed a series of amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act) to uplift the security and resilience of Australia’s critical infrastructure.

The owners and operators of critical infrastructure will be required to identify and take steps to minimise or eliminate risks that could have a ‘relevant impact’ on the asset. This will include managing insider risks through measures such as background checking.

[2] Transport to Security Outlook to 2025, Department of Infrastructure and Regional Development (2017).

[3] Australian Cyber Security Centre Annual Cyber Threat Report, July 2020 to June 2021, Australian Cyber Security Centre (2021)

At present, in the transport sector, the management of security identification cards is a distributed function across industry and government entities with AusCheck only responsible for background checking services.

AusCheck also houses the ASIC and MSIC issuing body for government agencies, operating as delegated by the Comptroller-General of Customs.[4]

AusCheck's broadening role

In this context, AusCheck is ready to evolve into the Commonwealth's preferred background checking service for employees and volunteers in critical infrastructure and those involved with other activities – such as major national events (MNEs) – where insider risks can compromise security and community safety.

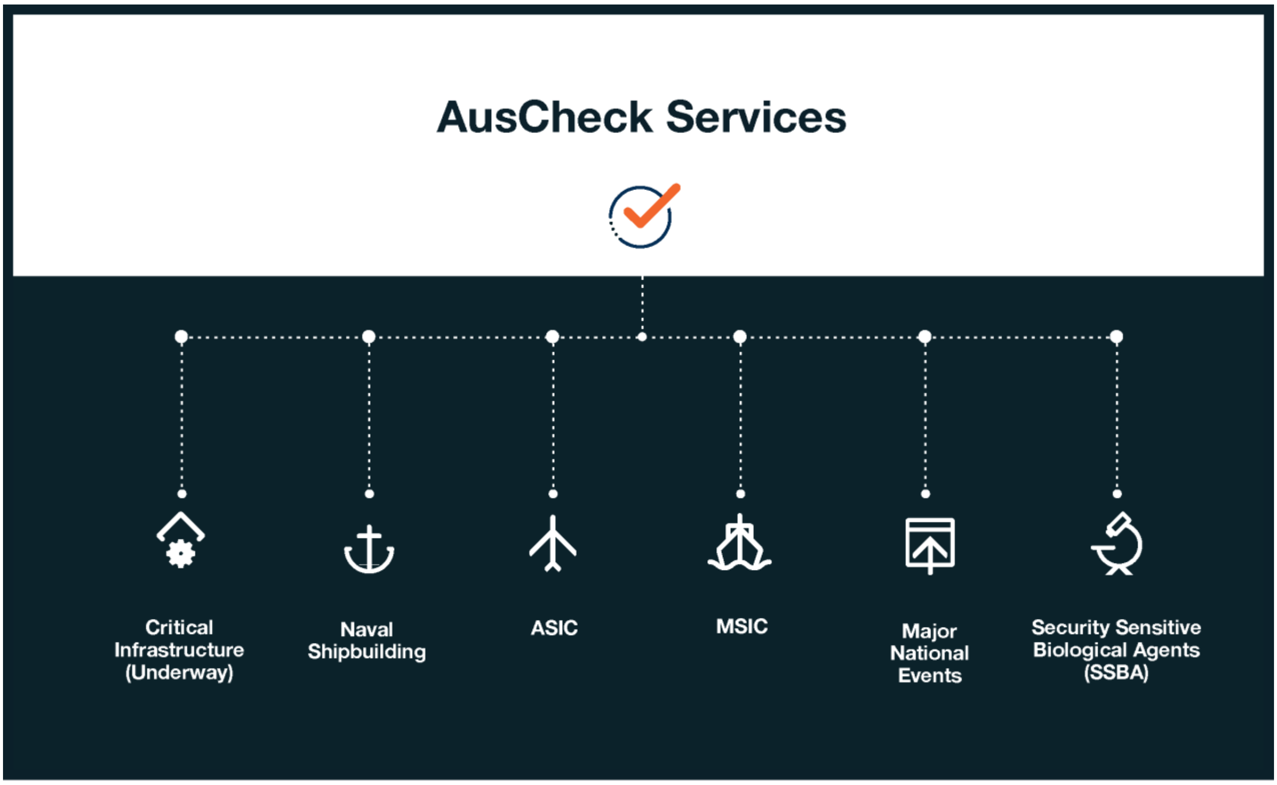
While AusCheck was initially created to undertake background checking for the transport sector, it is already engaged in supporting MNEs, and is about to start background checking for the defence industry's naval shipbuilding enterprise.

The single issuing body reform

The Department has developed a core capability model that can achieve the Government's objectives while also considering feedback provided by key stakeholders. This model incorporates changed roles for AusCheck, commercial partners, applicants and existing card holders, employers and facility operators.

The expanded services to be managed by AusCheck are summarised in Figure 1 below.

Figure 1: The expanding scope of AusCheck services


AusCheck Services
Critical Infrastructure (Underway)
Naval Shipbuilding
ASIC
MSIC
Major National Events
Security Sensitive Biological Agents (SSBA)

[4] Aviation Transport Security Regulation 6.1 (2005), Maritime Transport and Offshore Facilities Security Regulation 6.07P (2003).

Each of these background checking schemes has unique requirements and governing law. The AusCheck background checking service that will continue to support each security identification scheme is governed by the AusCheck Act, the *AusCheck Regulations 2017* (AusCheck Regulations), the *SOCI Act and the Security Sensitive Biological Agents* (SSBA) *Standards* as mentioned in the *National Health Security Act 2007*.

Future directions

As reforms proceed, a significant benefit for government, stakeholders and the community will be AusCheck's ability to implement more effective and efficient practices in security identification services across the range of schemes it administers in support of Australia's national security.

We anticipate improvements in AusCheck's capabilities could be made in a number of areas. Most notably we intend to explore:

- Implementing mobile application/s to support both applicants/card holders and industry users of our services
- Adopting the Department's identity resolution approach, moving to 100% biometric collection across all schemes managed through AusCheck
- Making ASICs/MSICs and similar credentials electronically verifiable through the Face Verification System (FVS)
- Considering using a digital credential service which would be complementary to physical cards, and
- Providing system changes to a legislative change program that aligns regulated activity (e.g. user authentication through myGovID).

Why do we need to change the ASIC and MSIC schemes?

The ASIC and MSIC schemes ensure that those who require unescorted access to secure areas of security-controlled airports, security-regulated seaports and offshore oil and gas facilities have passed mandatory background checks and do not present a significant risk to transport infrastructure and operations. The schemes also ensure the integrity of other key workers with the ability to affect security controlled spaces, notably through air cargo shipments and the issuing bodies themselves.

Private sector issuing bodies are currently responsible for issuing the majority of ASICs and MSICs to individuals across Australia.

The current regulatory model requires Government intervention and regulatory oversight. There are inherent vulnerabilities in the current arrangements that are undermining the integrity of the schemes. These were set out in a Regulatory Impact Statement issued in August 2021, outlining referenced non-compliance from issuing bodies across each stage of the ASIC and MSIC issuing processes including with identity verification, confirming operational need, card production and card return.[5]

[5] Department of Home Affairs 2021, Issuing body reform for the aviation and maritime security identification card (ASIC and MSIC) schemes: Regulation Impact Statement for Second Pass Final Assessment 2021. Regulation Impact Statement for Second Pass Final Assessment 2021, Department of Home Affairs.

How will we get there?

AusCheck’s Core Capability Model being delivered for transition

AusCheck’s Core Capability Model will operate while issuing bodies transition to AusCheck. It includes the following stakeholder groups undertaking a range of functions as described below and in Figure 2 (overleaf). Applicants and card holders, employers and facility operators will access the AusCheck Issuing Body’s online portal via the Australian Government’s Digital Identity provider, myGovID[6].

- **AusCheck**

  Responsible for processing applications, authorising ASICs/MSICs for applicants and undertaking application quality assurance. AusCheck will also maintain card and applicant records. Service Desk functions and operating hours will be expanded in AusCheck to assist all user groups accessing the portal. AusCheck will also continue to conduct background checks.

- **Applicants and card holders**

  Responsible for submitting an application for an ASIC/MSIC and meeting application requirements (e.g. attending an in-person identity verification appointment). As cardholders, they will be obliged to notify AusCheck about any change of circumstances associated with the card (e.g. lost/damaged cards, change of name, change of job, etc.). They are also responsible for returning expired, cancelled and/or damaged cards.

- **Employers**

  Employers will provide endorsement of the operational need of ASIC/MSIC applicants. Notifying AusCheck of changes in circumstances remains a card-holder responsibility, but employers will also be able to advise of changes in circumstances during the life of the card. These might involve notifying of lost or damaged cards on behalf of the card holder, suspension or termination of employment or periods of long-term leave. Employers may also provide assistance to the employees to submit the application for an ASIC/MSIC.

- **Facility operators**

  Responsible for managing access control and sponsoring employers linked to their facility. They can also contribute to the management of card events during the life of the card (e.g. lost card, cancellation/ suspension, long-term leave). Facility operators will be able to verify an issued card and track the status of any existing application. Facility operators will also be employers for their own staff and contractors.

- **Commercial partners**

  The Department will enter into a commercial arrangement with a nationally dispersed partner who will be responsible for undertaking in-person identity verification of ASIC/MSIC applicants. The Department will also engage a separate commercial partner who specialises in the production and distribution of identification cards that meet national security standards (etc). Commercial arrangements with both partners will be in line with Commonwealth Procurement Guidelines.

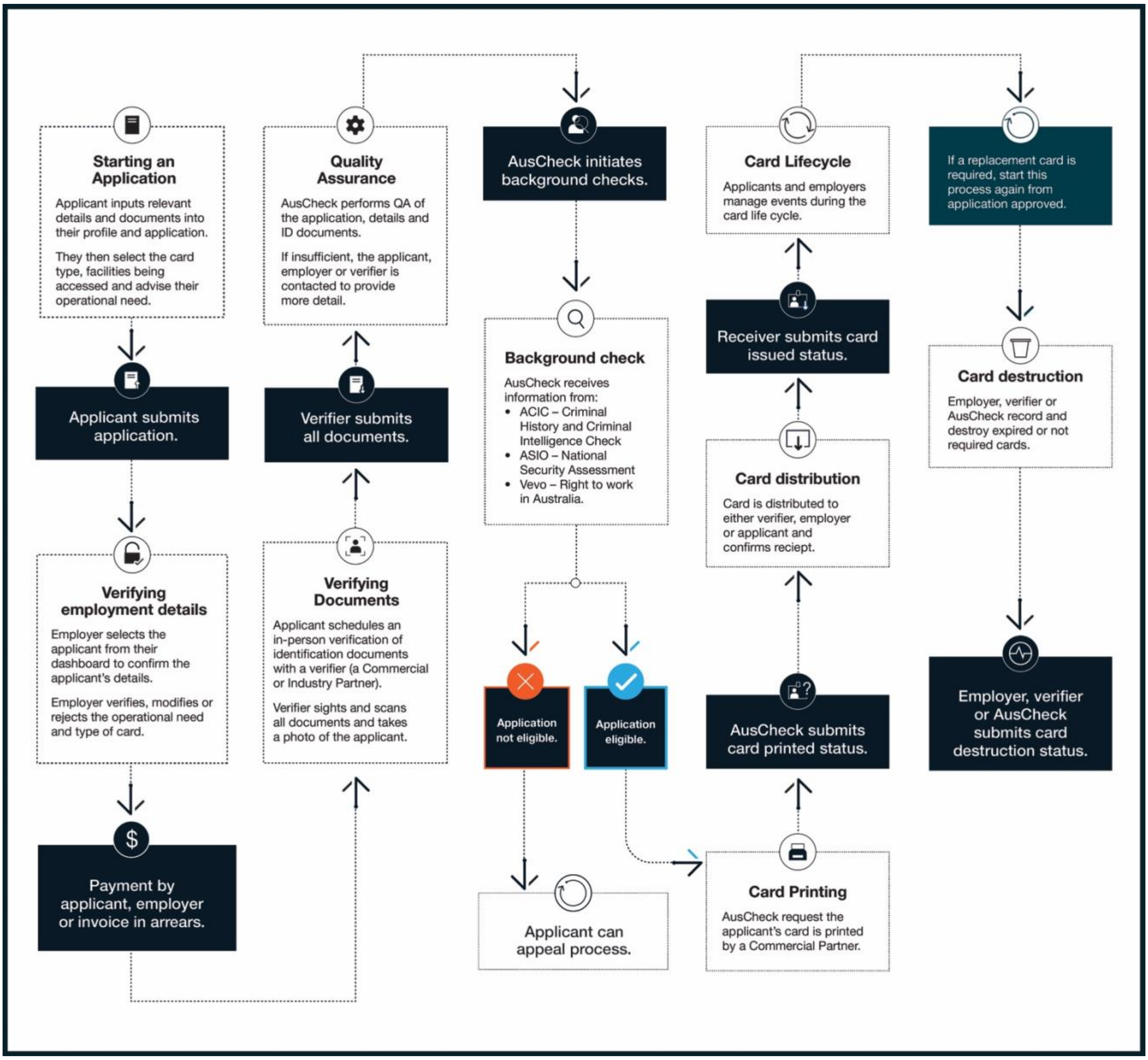
[6] myGovID is a person’s Digital Identity which can be used to access a range of government online services – mygovid.gov.au

- **Industry partners**

  AusCheck may engage industry partners to undertake in-person identity verification of applicants, where this service cannot be fulfilled by the Department's commercial partner. This role will be supported on an 'industry partner opt-in' basis. The risk assessment and legal framework for industry partners is still under development, but we expect that the management of industry partner relationships will be through contractual arrangements rather than regulations.

  Individual industry partners will be subject to an approval process that will include strict compliance requirements and a risk assessment conducted by AusCheck. Industry partners will need to be a transport service or a transport facility operator with a demonstrated and direct connection to the protection of critical infrastructure.

Figure 2: Core capability model process flow


Starting an Application
Applicant inputs relevant details and documents into their profile and application.
They then select the card type, facilities being accessed and advise their operational need.
Applicant submits application.
Verifying employment details
Employer selects the applicant from their dashboard to confirm the applicant's details.
Employer verifies, modifies or rejects the operational need and type of card.
Payment by applicant, employer or invoice in arrears.
Quality Assurance
AusCheck performs QA of the application, details and ID documents.
If insufficient, the applicant, employer or verifier is contacted to provide more detail.
Verifier submits all documents.
Verifying Documents
Applicant schedules an in-person verification of identification documents with a verifier (a Commercial or Industry Partner).
Verifier sights and scans all documents and takes a photo of the applicant.
AusCheck initiates background checks.
Background check
AusCheck receives information from:
• ACIC – Criminal History and Criminal Intelligence Check
• ASIO – National Security Assessment
• Vevo – Right to work in Australia.
Application not eligible.
Application eligible.
Applicant can appeal process.
Card Lifecycle
Applicants and employers manage events during the card life cycle.
Receiver submits card issued status.
Card distribution
Card is distributed to either verifier, employer or applicant and confirms reciept.
AusCheck submits card printed status.
Card Printing
AusCheck request the applicant's card is printed by a Commercial Partner.
If a replacement card is required, start this process again from application approved.
Card destruction
Employer, verifier or AusCheck record and destroy expired or not required cards.
Employer, verifier or AusCheck submits card destruction status.

NB: For the purpose of this Discussion Paper, this conceptual model has omitted certain workflows, such as provision of alternative IDs, ASICs/MSICs for under-18s or 14s, provision of discretionary cards, and payment process.

Assurance framework for Industry Partners

In proceeding with an industry partner model, the Department will establish an approval process to assess the suitability of potential partners. The priority for the Department will be establishing sound assurance that appointment of industry partners will not lead to vulnerabilities experienced with the existing issuing body arrangements.

There will also be an assurance process involved in appointing commercial partners. That process is not canvassed in this Discussion Paper because it will be managed through the Commonwealth Procurement processes.

The framework we propose for considering potential industry partners is discussed below and summarised in Figure 3 (overleaf).

- **Ability to meet service standards**

  Any services to be delivered by a commercial partner will need to meet the same outcomes, quality and timeliness standards as services provided through AusCheck and its commercial partners. The exception to this may be that an industry partner may not need to provide services nationally.

- **Security posture and culture**

  Prospective industry partners must be able to demonstrate their commitment to continuous improvement in security (including cyber security) strengths and how well they can prepare for, prevent, respond to and recover from ever-changing risks. A prospective industry partner will also need to be able to demonstrate their ongoing connection to the protection of critical infrastructure through a regulatory means, such as maintaining a Maritime Security Plan or Transport Security Program.

- **Compliance history**

  Prospective industry partners must be able to demonstrate a track record of compliance. They must specify their internal governance mechanism, demonstrating how past compliance and future service assurance requirements have been and will be met.

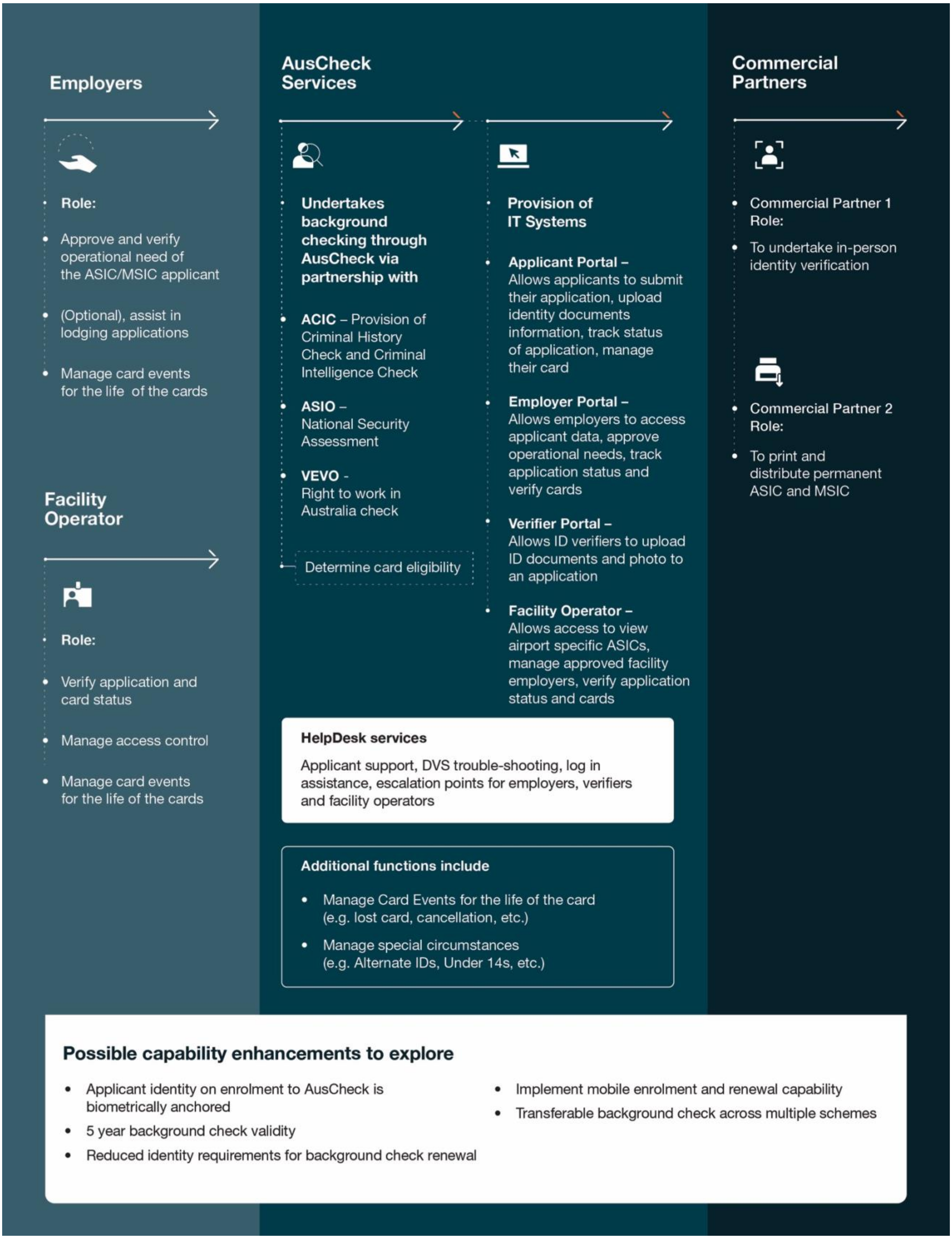
- **Capability, capacity and reach**

  This will be used to determine the prospective industry partner's ability to deliver the intended service in accordance with AusCheck's standards. This will include technical capability and capacity, as well as resourcing levels and service standards. Prospective industry partners must also demonstrate a service reach relevant to the card applicants/card holders they will serve, which may include servicing regional and remote facilities.

- **Quality assurance**

  The potential partner will need to demonstrate that their quality control systems, business continuity and business recovery arrangements can assure ongoing service delivery which meets industry and Government standards. This will most likely entail demonstrating how these standards will be met, as well as ensuring that the products and services are fit for purpose, well-made, uniform, and safe.

Figure 3: AusCheck Issuing Body Core Capability Model



Employers

- Role:
- Approve and verify operational need of the ASIC/MSIC applicant
- (Optional), assist in lodging applications
- Manage card events for the life of the cards

Facility Operator

- Role:
- Verify application and card status
- Manage access control
- Manage card events for the life of the cards

AusCheck Services

- **Undertakes background checking through AusCheck via partnership with**
- **ACIC** – Provision of Criminal History Check and Criminal Intelligence Check
- **ASIO** – National Security Assessment
- **VEVO** - Right to work in Australia check

Determine card eligibility

- **Provision of IT Systems**
- **Applicant Portal –** Allows applicants to submit their application, upload identity documents information, track status of application, manage their card
- **Employer Portal –** Allows employers to access applicant data, approve operational needs, track application status and verify cards
- **Verifier Portal –** Allows ID verifiers to upload ID documents and photo to an application
- **Facility Operator –** Allows access to view airport specific ASICs, manage approved facility employers, verify application status and cards

HelpDesk services

Applicant support, DVS trouble-shooting, log in assistance, escalation points for employers, verifiers and facility operators

Additional functions include

- Manage Card Events for the life of the card (e.g. lost card, cancellation, etc.)
- Manage special circumstances (e.g. Alternate IDs, Under 14s, etc.)

Commercial Partners

- Commercial Partner 1 Role:
- To undertake in-person identity verification
- Commercial Partner 2 Role:
- To print and distribute permanent ASIC and MSIC

Possible capability enhancements to explore

- Applicant identity on enrolment to AusCheck is biometrically anchored
- 5 year background check validity
- Reduced identity requirements for background check renewal
- Implement mobile enrolment and renewal capability
- Transferable background check across multiple schemes

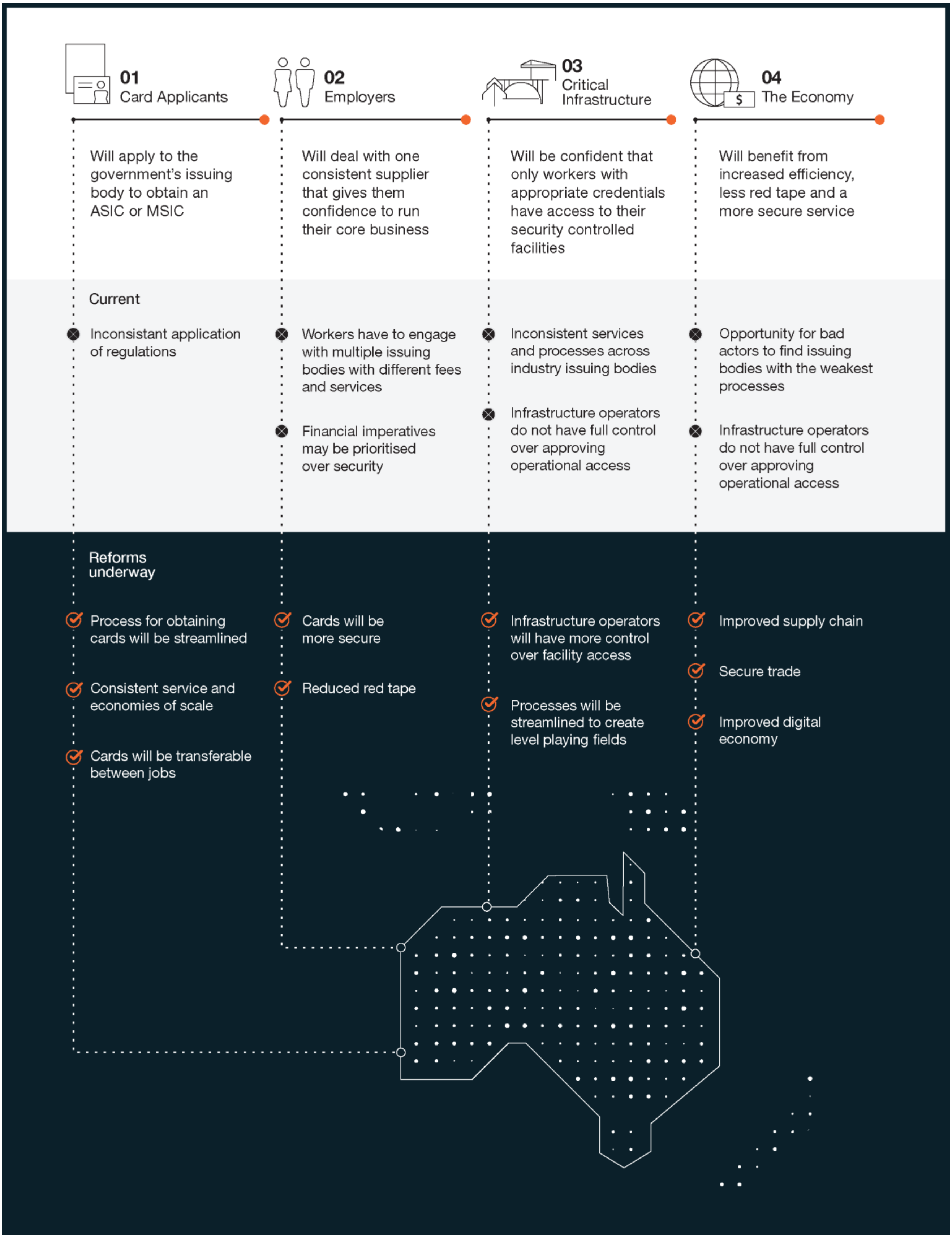
Key benefits of our proposed approach

Key benefits of the AusCheck Core Capability Model over the current model are set out below:

- The application process will be streamlined and data integrity strengthened. There will be an internationally-accessible online cyber-secure portal for applicants/card holders with a key focus on providing a self-service function. This will allow an individual to submit and track their applications, including operational need, and submit any change of circumstances over the life of the card.
- Employers will have access to the online portal to determine and approve operational need and card type for their workers.
- Facility operators will have access to the online portal to view and manage relationships between their sponsored employer groups, to verify currently issued cards and to track the status of an application for an individual.
- A process will be in place to ensure employers have a legitimate relationship with particular facilities before permitting access to certify operational need.
- With a single database managed by AusCheck, data security, access control, data integrity and cyber security controls will be strengthened. Most risks associated with ASIC and MSIC data security will be transferred from industry to the Department.
- Card quality and integrity will be strengthened. The Department will engage with commercial partners to undertake card production and distribution, and in-person identity verification. The selection of commercial partners will be based on Commonwealth Procurement Guidelines and criteria that can deliver maximum value to the Department while managing a robust security posture.
- There will be appropriate system access for commercial partners to enable trusted data sharing from AusCheck, to enable in-person identification verification and card production processes.
- Employers, commercial partners or facility operators will receive the ASIC/MSIC before passing it to the applicants. Applicants may also elect to receive their card directly to their residential address.
- Facility operators will remain responsible for access-control arrangements. Card production on current encodable card stock will be available to ensure continuity of existing service.
- Employers and Facility Owners will be able to assist card-holders through the initial application process, implement and manage access control to their site and manage any change of circumstances through the online employer portal. This will not require a formal industry partnership arrangement.

Figure 4 (overleaf) illustrates how these benefits of a single issuing body resolve the concerns about the operation of the current issuing body schemes.

Figure 4: Benefits of the issuing body reform



	01 Card Applicants	02 Employers	03 Critical Infrastructure	04 The Economy
	Will apply to the government's issuing body to obtain an ASIC or MSIC	Will deal with one consistent supplier that gives them confidence to run their core business	Will be confident that only workers with appropriate credentials have access to their security controlled facilities	Will benefit from increased efficiency, less red tape and a more secure service
Current	⊗ Inconsistant application of regulations	⊗ Workers have to engage with multiple issuing bodies with different fees and services ⊗ Financial imperatives may be prioritised over security	⊗ Inconsistent services and processes across industry issuing bodies ⊗ Infrastructure operators do not have full control over approving operational access	⊗ Opportunity for bad actors to find issuing bodies with the weakest processes ⊗ Infrastructure operators do not have full control over approving operational access
Reforms underway	✓ Process for obtaining cards will be streamlined ✓ Consistent service and economies of scale ✓ Cards will be transferable between jobs	✓ Cards will be more secure ✓ Reduced red tape	✓ Infrastructure operators will have more control over facility access ✓ Processes will be streamlined to create level playing fields	✓ Improved supply chain ✓ Secure trade ✓ Improved digital economy

So where are we now?

What industry has told us

The Department undertook initial industry engagement through one on one discussions with all issuing bodies in February and March 2022. Site visits to issuing bodies, industry participants and other stakeholders continued from April 2022 until September 2022, to understand the concerns, issues and opportunities of transitioning to a single issuing body. Below are some of the most common issues expressed:

- **Transition Timeframe**
  Issuing bodies sought clarification on the transition timetable. Some issuing bodies voiced a preference for a longer transition period (e.g. ten years). Several issuing bodies, on the other hand, are content with a moderate transition period (e.g. 6–18 months), while a minority of issuing bodies are seeking less than six months' notice.
  We propose concluding the transition of all issuing bodies to the single issuing body by 30 June 2025.
- **Future operating model**
  One of the main concerns raised was the single issuing body's operating model. The existing issuing bodies are likely to face changes to their business operations, workforce implications, financial consequences, and stakeholder engagement, and they will need to mitigate these consequences. Issuing bodies want to know more about the future operating model and many expressed an interest in participating in any collaborative process.
- **Co-design process and business impact on the transition**
  Issuing bodies and industry participants want to know how the future operating model will be formed, as well as what kinds of system design or business process modifications they'll have to manage during and after transition. Further, issuing bodies want to know more about the co-design process, such as what aspects of operations will be covered and how end-to-end business process will be managed.
  The detailed co-design process is expected to begin in late 2022, providing issuing bodies the opportunity to contribute to defining the end state operating model of the single issuing body.
- **Meeting the demand and service expectations**
  Issuing bodies are in charge of managing the existing volume and demand for services, supported by a number of partnerships, agreements, and service contracts. This transformation will need to be able to satisfy demand and meet the employers' and card holders' expectations. Some issuing bodies raised the need for after-hours services for their shift workers. Similarly, issuing bodies flagged that some applicants and card holders have limited IT skills and require support.
  As part of the co-design process we will confirm and agree on a set of industry standards and key performance indicators that the Department will meet.
- **Remote/regional facility locations**
  The geographical scope of issuing bodies' services extends to some remote and regional places around Australia. There are concerns that moving to a single, centralised issuing body may impede the timely and efficient supply of services to remote and regional facilities, including offshore facility operators and other fly-in-fly-out (FIFO) workers. Some third-party issuing bodies have a very broad reach and any transition planning activities will need to account for the increased impact and service reach across a vast geographical region and user base.
  The proposed workshops as part of co-design will address some of these issues and we will develop proposals to ensure that service delivery standards are met.

- **Communication approach**
  Several issuing bodies raised concern about the lack of communication tools currently available to them during the transition process. Issuing bodies require information that they can relay to their workers, partners, and other stakeholders as the future operating model is built.
  We will develop communication tools which exiting issuing bodies can use to inform their stakeholders of relevant information.
- **Data sharing and storage**
  Some issuing bodies expressed concerns about how data will be shared to manage any risks posed by prospective or current card holders as services are transitioned. Employers may be required to conduct additional security checks on cardholders in certain circumstances. Further, there are worries about the security and storage of data, records, and physical files.
  There is an online portal for the applicants, card holders and employers that will allow access to certain-personnel records for additional security assessment if required by the employers. This will be in line with privacy and legislative permissions.
- **Access control**
  Questions about how the security card will interoperate with facility access controls were raised. Some issuing bodies provision encodable security cards for access control in single or multiple sites. Queries were raised concerning the encoding feature, the issue of temporary cards, and other measures to assure access control might be accomplished.
  Access control remains an industry responsibility; not that of the Government. The single issuing body will produce security identification cards. We will provide an applicant with an ASIC/MSIC printed on an encodable card stock if/as requested by the employer. Any additional expenses associated with this service have yet to be agreed.
- **Financial impact**
  Some issuing bodies have raised concerns that transitioning to a single issuing body would result in commercial losses for their businesses. Issuing bodies' investment in physical assets, maintenance of current security card production infrastructure, implementation of cyber security efforts, and investment in future expansions of their services are all contributing to this concern. Further, if business activities are lost, some employees may lose their jobs.
  We will work with all issuing bodies to manage the impact to their business. Transition support teams consisting of a number of specialised resources including communications, training, change management, project support, as well as an actuary, will ensure that all issuing bodies are well informed of when the optimal transition window specific to their circumstances may be.

Call for response

1. Are there important issues from your perspective which are not captured by this summary?

Our service standards

AusCheck will operate a national Service Desk and secure web portal to support applicants, card holders and employers. The Service Desk will operate from 7am Eastern Standard Time to 7pm Western Time, providing an extended service window as the norm. Further, we will explore the option to locate Service Desk personnel in metropolitan centres in proximity to industry centres.

We are still considering if the operating model should allow employers and facilities to retain the ability to produce and issue temporary cards. Employers and facilities will retain the ability to print visitor identification cards (VICs) and where applicable temporary aircrew cards (TAC) to ensure that urgent out-of-hours requirements can be met. To assist with the issue of VICs and TACs employers and facilities will be able to confirm the cardholders' card status using the portal. A replacement permanent card will then be printed and distributed by AusCheck. The applicant, employer and facility operator portals will be accessible 24/7.

We recognise that many card applicants will require support and assistance, and this will be managed by our national Service Desk offerings as well as by the applicant's employer. Complex cases will be managed through our Service Desk and escalated to the relevant level of support based on the individual requirements.

AusCheck is committed to providing professional and consistent service standards. We will treat your dealings with us in confidence and:

- Act in a helpful and professional manner
- Provide an accurate, concise and well-considered reply in plain English
- Where requested, provide an update of application progress in 28 business days, where completion in 5 business days is not possible
- Tell you before commencing work if there is a fee for the services you have requested and provide an estimate of the overall fee
- Where we are unable to assist, do our best to refer you to the most appropriate agency.

Our service levels will include:

- IT Portal availability: >99%
- >90% of background checks completed by our partners in 6 weeks
- Card application decisions: 98% of applications finalised in 5 working days of background checks being returned by our partners
- Changes of circumstances determined in 5 working days.
- Card issue: >80% of cards received in 10 calendar days of decision
- Service Desk: >80% of calls answered in 2 minutes
- First-time resolution: >80% of matters resolved on first enquiry, and >95% of enquiries resolved in 7 days (note: some processes, such as discretionary cards, will require longer periods to finalise).

The AusCheck Service Charter will be updated in preparation for transition and discussed further as part of co-design activities.[7]

Call for response

2. Will issues for industry arise from these standards, and if so, what are the service standards which apply to your current arrangements?

[7] AusCheck Service Charter, Cyber and Infrastructure Security Centre website.

What will the single issuing body mean for industry members?

How will AusCheck support industry, card applicants and card holders?

- AusCheck will support those involved with card applications and management with unified national support arrangements and ready access to necessary information.
- The business systems will support portals for applicants and card holders, employers and facility operators, interfaces with commercial partner systems and cyber-secure Application Programming Interfaces (APIs) for industry participants to use – if they wish – with internal systems.
- Nationally consistent business processes will avoid the current multiple handling and duplicated arrangements. A national business system will be able to work more efficiently for the benefit of all users.
- To support the transition, AusCheck is establishing a dedicated team to work with issuing bodies in coordinating planning and management of the reform. The current AusCheck Issuing Body is being progressively expanded in preparation for the transition process. Additional resources are also being dedicated to establishing and managing commercial partnerships – and scheme assurance more broadly.

What will change for current issuing bodies and commercial service providers?

Issuing body responsibilities will transfer to AusCheck.

- There will be a single ‘point of truth’ for all card and AusCheck information, and former issuing bodies will not need to hold on-site physical or electronic files relating to issuing body functions.
- Cyber-secure portals will be available to applicants and card holders, employers and facility operators to manage their scheme functions and confirm application status when required.
- A national network will be in place for identity verification.
- A national network will be in place for permanent card production and distribution to employers, facility operators or an applicant, addressing issues in the current model related to card production standards.
- Employers will retain the ability to locally print VICs, TACs, and possibly temporary ASICs/MSICs.
- Employers will be in practical control of validating operational need.
- Regulatory oversight for issuing body functions will not be needed; management of commercial partners will be undertaken by AusCheck.
- In relation to ASIC and MSIC data, former issuing bodies will no longer be required to comply with cyber security directives from the Department of Home Affairs. This data will be retained by AusCheck under a single issuing body structure. Employers and facility operators will remain in control of access cards and access control systems for their facilities, and may assist with issuing cards to applicants.

The challenges we face along the way

We acknowledge the feedback provided from industry indicating that the AusCheck core capability model may need to be adjusted to meet use cases for service standards and service delivery. The case studies embedded in this paper already highlight some of the complexities involved.

While it is unlikely that the new arrangements can reflect every practice adopted by each of the current issuing bodies, we will work with industry to ensure that the approaches we have described deliver the required service standards.

Constraints

Implementation of expanded AusCheck services will be subject to the following constraints.

- **Consistency with the Government's announced intentions**

  In developing its approach, the Department is ensuring that the proposed solutions are consistent with the Government's decisions – most notably the single issuing body reform. It is also a priority that the approach materially improves the risk profile associated with current arrangements – notably addressing vulnerabilities with cyber security, card integrity and records management standards.

- **Critical dates**

  By June 2023, AusCheck's issuing body system will be ready to accept ASIC and MSIC applications from members of the public using cyber-secure portals. It is anticipated that the earliest possible transition for the first issuing body will be from 1 July 2023.

  It may be prudent to allow some lag to accommodate training and final preparations before any high-volume issuing body transitions. The Department will need to settle on a date for achievement of a single issuing body, which will be influenced by industry feedback to this paper.

  At present, the date by which we intend to complete the transition is 30 June 2025, subject to consultation.

- **Regulatory compliance**

  During the transition, all regulatory compliance as defined in the *Aviation Transport Security Regulations 2005* (ATSR) and the *Maritime Transport and Offshore Facilities Security Regulations 2003* (MTOFSR) will be maintained.

  However, once the transition to AusCheck is completed, it is expected that we will discover opportunities to streamline the regulatory framework.

  The issuing body model is expected to be replaced by a new regulatory framework, whether in the AusCheck Regulations or the ATSR and the MTOFSR.

- **Risk management**

  A key goal of the move to the single issuing body is to reduce the prospect of vital aviation and maritime infrastructure being exposed to security risks. As a result, during the implementation and transition decision-making process, any security risk exposure will be minimised and integrity of the schemes will be strengthened.

  The Department appreciates that while risk control is fundamental, solutions also need to be workable. Your feedback will help shape the approach to deliver both outcomes.

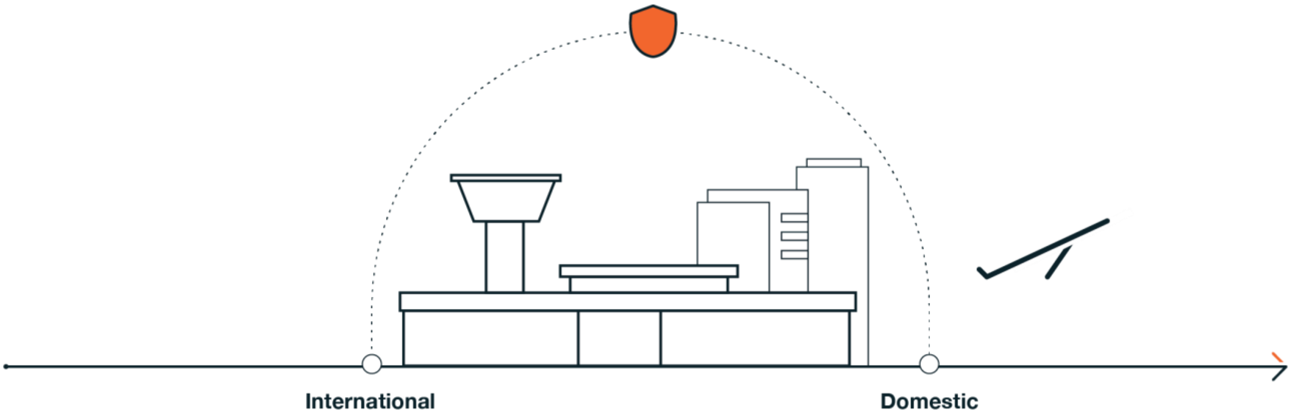
- **Service-level standards**

  It is critical to ensure that industry needs, such as service standards, card production, card distribution, and other related business processes, are met as the transition to the single issuing body takes place. This will include thorough preparation and engagement with industry stakeholders in order to capture desired service levels, business processes, and establish strategies to ensure service standards are met.

  We see a strong service culture in AusCheck and a well-designed core capability model as key elements in achieving this.

Case Studies

Case Study 1: Designated airport



Designated airport

Current

This large airport is an approved issuing body and facility, operating domestic and international facilities in a metro area with large ASIC demands. As an international gateway they facilitate extensive quantities of both passenger and freight transport for the region.

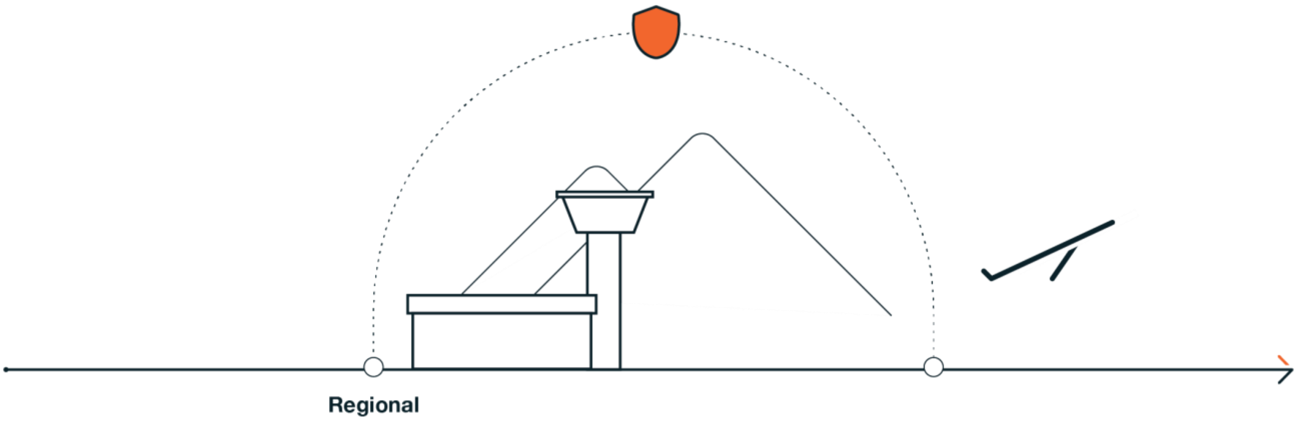
The airport operates large service centres (international & domestic) that provides support for a very large number of airport and aircrew roles. These service centres are not only responsible for ASICs, but administer airport access control cards, and VICs. As a metropolitan facility, they benefit from reduced distribution times at the front of the supply chain for inputs, products and services.

An employee at the airport completes an ASIC application form via the service centre website which triggers a requirement to undertake mandatory security awareness and site induction training prior to their application being sent to AusCheck for background checking. Once approval has been obtained, all printing and production is completed on-site and the ASIC is provided to the employee. As an issuing body, the airport is mandated to maintain security and regulatory compliance in accordance with their ASIC Program.

Future

We believe this facility operator can maintain control of card applications by not validating operational need until the local training has occurred. Some applicants will want support in lodging card applications via the online applicant portal, but others will use the portal effortlessly. Given the metropolitan location, card production by AusCheck's commercial partner on encodable card stock, issued to applicants via the airport facility operator, should help retain the strong operational control required. This will allow the airport to manage the completion of their necessary training requirements and provision electronic access control on the ASIC before it is handed to the applicant.

Case Study 2: Regional airport



Regional airport

Current

This airport is an issuing body operating a fast-growing business that has transitioned in the last ten years from domestic-only to include international flights. Initially receiving seasonal international services, they now receive year-round services, with seasonal peaks. The current terminal building predominantly caters for domestic operations with a 'swing gate' arrangement for international travel. Staffing at the airport is fewer than 100 employees and must be able to adapt to significant numbers of flight crews who are required to access the facilities throughout the week.

For an employee at the airport, the current process for application is through completing a printed hard copy form that is then checked against operational need, and documents verified, prior to being sent for background checking. AusCheck provides the background check outcome and a third-party partner prints the card before distribution to the successful applicant. Being a regional area, the airport can experience distribution and supply chain delays. They value being able to provide face-to-face facilitation of the issuing body process, resulting in more efficient outcomes for compliance and applicants alike – seeing this process as an important element for their employee relationship management.

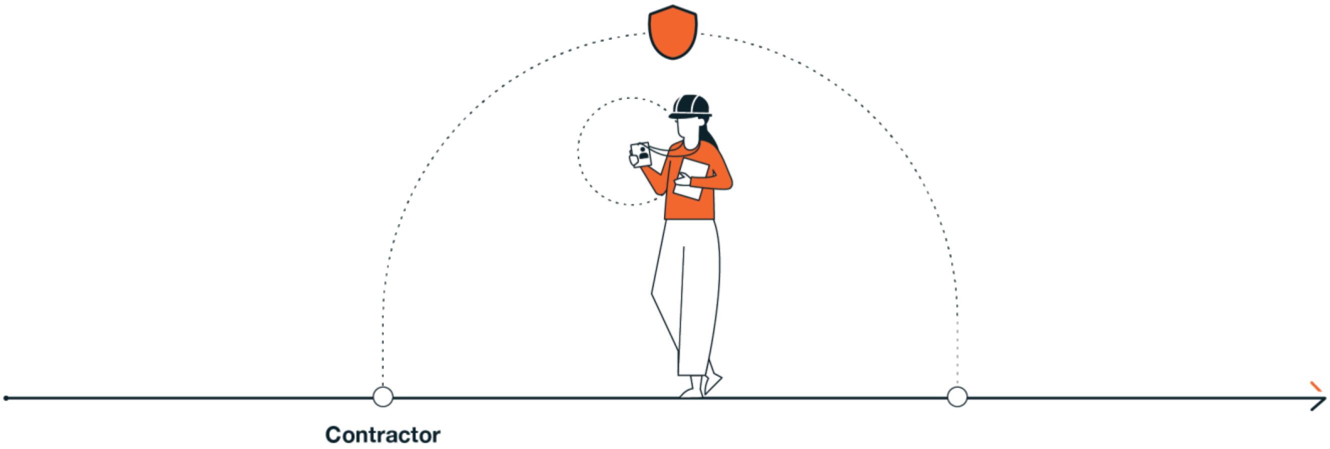
Future

This operator may have a case for verifying identity, although the AusCheck commercial partner may undertake this function. Industry partners will be subject to an approval process that may include strict compliance requirements, a risk assessment and business case. Issuing the card via the facility operator rather than the commercial operator would support a strong facility relationship with card holders.

Call for response

3. How would relying upon AusCheck's core capability affect your current operations, risk profile or service standards for issuing body functions?
4. Are there circumstances where cards issued through facility operators would be of benefit to you?

Case Study 3: Contractor



Contractor

Current

Lucy is a contractor operating in secure zones, and she requires a security identification card for her work. Lucy is a sole trader who would endorse her own operational need. To date she has received her card from a commercial issuing body not attached to critical infrastructure (major employer or facility). The card she was issued was then taken to the site manager for the facility to be coded for appropriate access.

Future

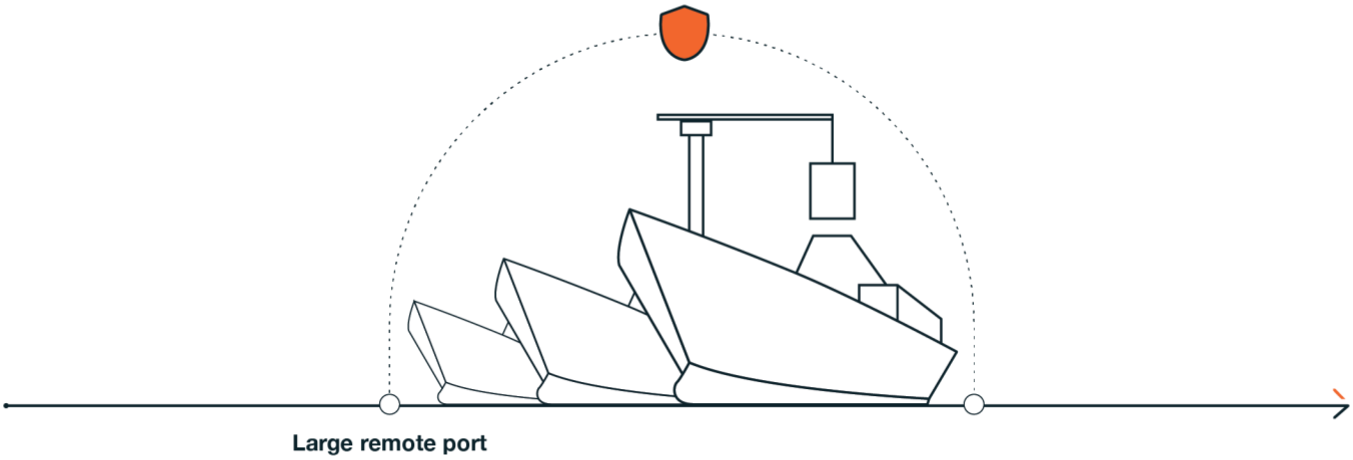
In the proposed arrangements, Lucy's company will have confirmed sponsorship through the facility operator which will support her operational need. While Lucy's identity will be verified by AusCheck's commercial partner and the card issued by the single issuing body, Lucy will still need to present to the facility operator for access control to be facilitated and to ensure she has completed the local induction and security training requirements.

The facility operator will still be responsible for managing any pre-requisite training or induction requirements, as well as provisioning access control. As different access control systems require different encodable card stock, the facility provider may wish to issue Lucy with a local access card in addition to her AusCheck issued security identification card.

Call for response

5. Do you believe that establishing a sponsored link between a facility and sole trader will support a facility operator in managing operational need, access control and training requirements for staff and contractors requiring access to their site?

Case Study 4: Large remote port



Large remote port

Current

This approved issuing body, a very large bulk goods facility operator on a global scale, operates and provides oversight for several ports in a remote regional area. They operate on a precision system built for efficiency and would be impacted by any delays in the MSIC process, such as distribution delays due their remote and regional location. They expect high service level standards and, to mitigate this delay, they operate an on-site issuing body service centre and card production facility.

An employee who requires an MSIC must apply through the port's website and complete mandatory security training before their application is sent to the AusCheck portal for background checking. Once the application is approved through AusCheck this is communicated to the port and the MSIC can be printed. The employee is then able to collect their MSIC from an on-site service centre. Port users have face-to-face interaction with the issuing body service centre, enabling them to receive in-person support and expedited service delivery.

Future

We think this operator may have a business case for supporting verification of identity, as well as card issuing. We think permanent card production by AusCheck's commercial partner is viable, as long as temporary cards can be printed locally, as outlined in the operator's Maritime Security Plan.

Managing a transition timeframe

We will structure transition by grouping issuing bodies into three distinct tranches. This will allow for a higher touch approach for transition and for us to ensure there are no disruptions to the aviation and maritime security sectors. We will commence on 1 July 2023 and conclude for all issuing bodies by 30 June 2025 (see Figure 5 overleaf).

- **Tranche 1 – 1 July 2023 to 30 June 2024**

  Low complexity issuing bodies

  Typically, issuing bodies who have a low number of cards on issue (i.e. less than 1,000 cards) or are low complexity, with little to no integration with other systems.

  These issuing bodies likely accept and process applications in a hard-copy format, manually transcribing data into their internal systems before lodging one-by-one with AusCheck background checking services. Their systems are completely stand-alone with access control, mandatory training and HR systems being managed separately.

  Removing the issuing body service from these operators will have minimal impact to the operations of their business, provided that they have access to a facility operator portal to validate cards and track the status of applications.

  We will need to explore partnering with transitioned industry operators to conduct identity verification on our behalf, while we finalise commercial engagement with a national identity verification provider.

  Printing and distribution of cards for applicants from this tranche will be managed by AusCheck's existing issuing body capability and is not reliant on the engagement of a commercial provider.

- **Tranche 2 – 1 January 2024 to 30 June 2025**

  Commercial issuing bodies

  Outside of their issuing body role these issuing bodies likely do not have a direct connection to the protection of Australia's critical infrastructure. Commercial issuing bodies are not a maritime or aviation industry participant and not necessarily regulated in ways other than under their status as an issuing body, as per the ATSR and/or the MTOFSR.

  By the commencement of Tranche 2, engagement with both the card production and distribution service provider/s, and the identity verification commercial provider/s will be established.

- **Tranche 3 – 1 July 2024 to 30 June 2025**

  High complexity issuing bodies

  These issuing bodies are likely to be large employer or facility operators who have a high volume of cards on issue, and complex system integrations in place.

  Systems supporting their issuing body operations are heavily integrated with HR personnel, electronic access control, vehicle booking and internal mandatory training systems.

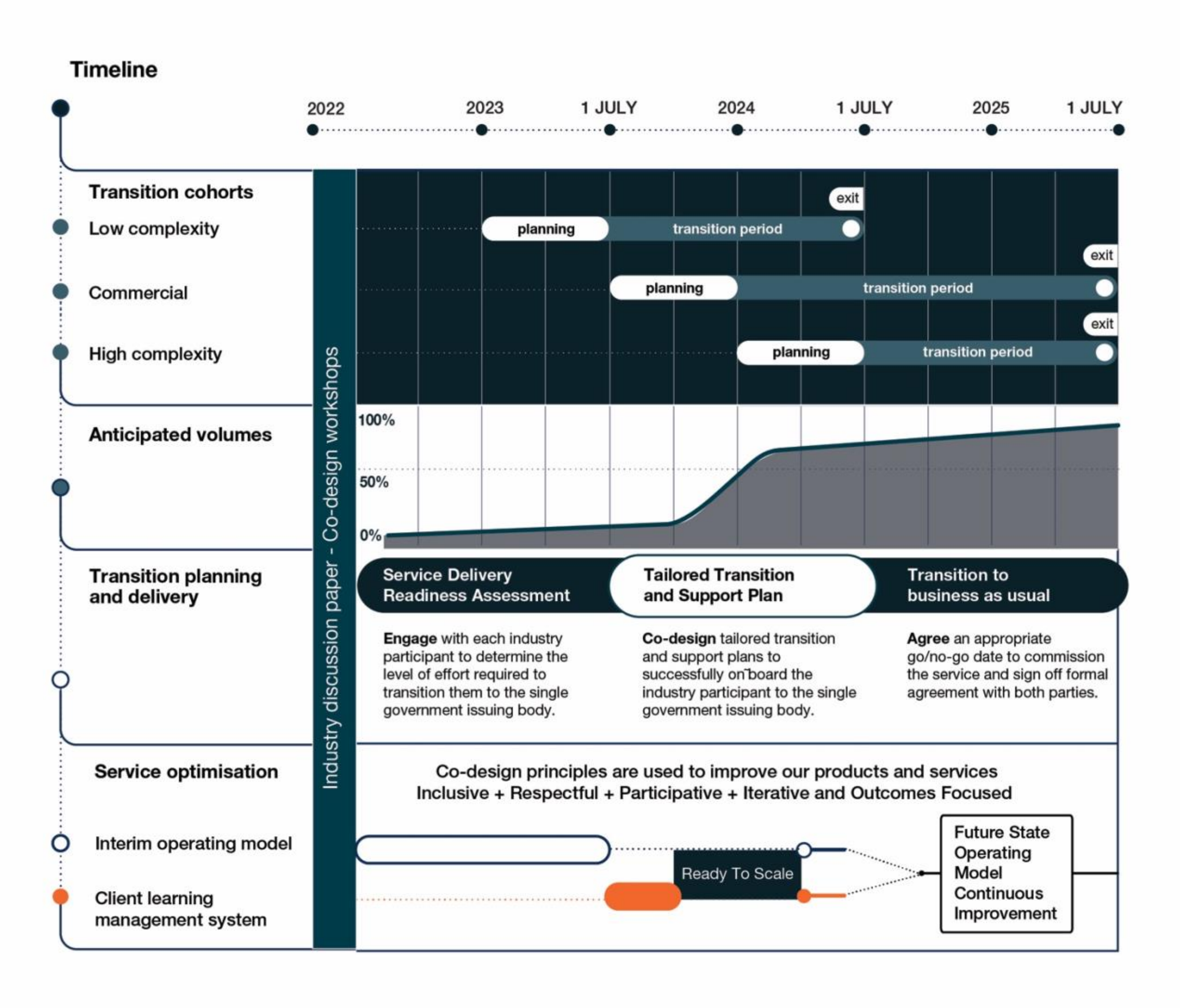
  These employer and facility operators will require additional support from the AusCheck Issuing Body to unpick the associated various complexities, and may require the development of cyber-secure APIs to support their operations.

  Identity verification and card production and distribution will be supported by commercially engaged providers.

We are aware that individual issuing body circumstances may require a different approach; for example, an issuing body's systems may be approaching end of life, which may suggest an earlier transition date is desirable. Likewise, if an organisation needs to make changes and manage integrations to support other business systems they might require a later date in order to minimise disruption.

We also anticipate that planning for peak workload requirements will affect timing; for example, aviation industry participants are likely to require a stable environment during school holiday or peak travel periods and some major events.

Figure 5: Single issuing body proposed timeline


Timeline
2022
2023
1 JULY
2024
1 JULY
2025
1 JULY
Transition cohorts
Low complexity
Commercial
High complexity
planning
transition period
exit
Anticipated volumes
100%
50%
0%
Industry discussion paper - Co-design workshops
Transition planning and delivery
Service Delivery Readiness Assessment
Tailored Transition and Support Plan
Transition to business as usual
Engage with each industry participant to determine the level of effort required to transition them to the single government issuing body.
Co-design tailored transition and support plans to successfully on board the industry participant to the single government issuing body.
Agree an appropriate go/no-go date to commission the service and sign off formal agreement with both parties.
Service optimisation
Co-design principles are used to improve our products and services
Inclusive + Respectful + Participative + Iterative and Outcomes Focused
Interim operating model
Client learning management system
Ready To Scale
Future State Operating Model Continuous Improvement

Call for response

6. Based upon our proposed transition timeline and tranches, where do you see yourself fitting?
7. If you have concerns about the proposed approach, what arrangements would you prefer and why?
8. What, if any, impacts would this transition timeline have on your resources (eg staff, equipment, contracts, investments etc)?

Operating during the transition period

During the transition phase there will be parallel streams of activity:

- AusCheck will continue to operate background checking services for all issuing bodies and other clients.
- A transition team will work with individual issuing bodies to plan and implement their transition to AusCheck. Issuing bodies will have allocated transition resources and a dedicated account manager to support planning and execution of their transition.
- The AusCheck Issuing Body will expand from its current clients – federal, state and territory government agencies – as issuing bodies transfer their work and are revoked. This will include an expanded Service Desk facility for applicants, card holders and industry participants.
- To support its operations, AusCheck will establish commercial partnerships for identity verification, and card production and distribution.
- Consultation and development of future post-transition arrangements will continue. This work will also include business system improvements to meet emerging needs.

Progressive revocation and the transition window for each issuing body

The Department will revoke individual issuing body authorisation in accordance with an agreed schedule. This will permit individual issuing bodies to minimise any costs associated with the transition and accommodate timing to the needs of each organisation. It will also permit the Department to ensure appropriate staffing is in place to support the change. We anticipate that an approach to phasing will be agreed during the co-design process that can accommodate individual issuing body preferences. Our proposal is outlined below.

Following individual issuing body co-design and agreement to a target end-date, transition for each issuing body is expected to take place over a window of 11 weeks:

- **Weeks 1–3:**

  Confirm readiness and exchange detailed information
- **Weeks 4–7:**

  Prepare for transition and cease acceptance of new applications at an agreed date; finalise any commercial arrangements such as purchase of Kinegram stamps and surplus card stock
- **Weeks 8–11:**

  Transition existing data and assets, undertake post-transition issue resolution, and sign-off on transition activities being complete.

In many cases, a shorter transition window may be possible. This will be explored as part of the planning for each transition.

Transition support

We will work with each issuing body to manage the impact to aviation and maritime security leading up to and during transition. We will provide specialist support to develop a specific transition plan for each issuing body based on their individual circumstances and requirements.

A transition team will be established to support each issuing body transition, including actuary, communications, training, and change management support officers. This team will work with each issuing body to agree their optimal transition time and negotiate a timeframe for transition. This will also consider an issuing body's card renewal period, leasing and contractual arrangements.

Call for response

9. What are your views on how the expenses for ASICs and MSICs (including background checks) should be funded: government appropriation, industry levy, individual user-pays/cost recovery fee, employer pays/cost recovery fee, etc?

Next steps

The Department will consult with stakeholders throughout the planning and transition periods. This will help us assess the impact of the proposed reforms and refine our development of the framework.

Responses to this paper

Throughout the paper there are *Call for response* topics, seeking your input on specific aspects of our proposed approach. These are topics where we believe your views can help us understand industry requirements and help us implement the Government's decision. You are also welcome to submit responses to any aspect of the reforms as set out in the Call for responses section at the end of this document. We will take careful note of all views we receive, and we will give priority to input that aids the successful implementation of the Government's decision.

Future engagement

The Department's future engagement will have three streams of activity:

- **Arrangements for managing individual issuing body transition:**

  This stream is for all issuing bodies and affected stakeholders.

  This will occur through individual discussions, co-design focussed on the transition, lessons learnt from the current scheme, and areas where commercial issuing bodies can add value to the work of the Department once transition is complete.

- **Arrangements for ongoing security identification card management:**

  This stream is for employers and facility operators who will sponsor and manage cards, as well as ongoing stakeholders.

  It will involve individual discussion, co-design activities and working groups.

- **Periodic Town Hall meetings:**

  These will keep all stakeholders informed and identify issues requiring attention.

The co-design process

Co-design is an iterative process for identifying and designing change. This Discussion Paper starts the formal co-design process for these reforms. Through a co-design process we will identify the best approach to implement the Government's decision.

For this reform, the focus of co-design will be:

- How change management and communication needs to work, including for current users of the issuing body and AusCheck services
- Service needs and standards, both during the transition and for ongoing service delivery
- High level business requirements for a successful transition
- Policy and regulatory settings following transition, and
- What further lessons can be learnt from experience with current arrangements.

We will hold in-person workshops in early 2023 to progress co-design, including substantive consideration of the approaches proposed in this Discussion Paper. Further detail about the co-design process will be provided following release of the Discussion Paper.

Call for response

10. Would your organisation like to participate in co-design workshops?
11. Do you have any views on representation in the co-design process?
12. Do you foresee a need for particular focus groups?
13. Are there proposed workshop topic/s which, in your view, might be missing or unnecessary?

Submissions

Closing date for submissions: 4 weeks from release

Submissions on this Discussion Paper are welcome from all stakeholders including aviation and maritime industry participants, government employees and officials, academia, and members of the public – but particularly those who will likely be directly affected by the reform.

We welcome written submissions in response to any or all of the consultation questions listed in this Discussion Paper. Please provide your submissions through the submission form on the AusCheck website, as well as any questions relating to the submission process, to: **IBREngagement@homeaffairs.gov.au**.

Submissions may be made public unless you specifically request the submission be kept confidential. The Department of Home Affairs is subject to the *Freedom of Information Act 1982* and may be required to disclose submissions in response to requests made under that Act.

The *Privacy Act 1988* establishes certain principles regarding the collection, use and disclosure of information about individuals. Any personal information respondents provide to the Commonwealth through submissions will be used for purposes related to the consideration of issues raised in this Discussion Paper, in accordance with the *Privacy Act 1988*. If the Commonwealth makes a submission, or part of a submission, publicly available, the name of the respondent will be included. Respondents should clearly indicate in their submissions if they do not wish their name to be included in any publication relating to this consultation that the Commonwealth may publish.

Appendices

Calls for response

1. Are there important issues from your perspective which are not captured by this summary?
2. Will issues for industry arise from these standards, and if so, what are the service standards which apply to your current arrangements?
3. How would relying upon AusCheck's core capability affect your current operations, risk profile or service standards for issuing body functions?
4. Are there circumstances where card issue through facility operators would be of benefit to you?
5. Do you believe that establishing a sponsored link between a facility and sole trader will support a facility operator in managing operational need, access control and training requirements for staff and contractors requiring access to their site?
6. Based upon our proposed transition timeline and tranches, where do you see yourself fitting?
7. If you have concerns about the proposed approach, what arrangements would you prefer and why?
8. What, if any, impacts would this transition timeline have on your resources (eg staff, equipment, contracts, investments etc)?
9. What are your views on how the expenses for ASICs and MSICs (including background checks) should be funded: government appropriation, industry levy, individual user-pays/cost recovery fee, employer pays/cost recovery fee, etc?
10. Would your organisation like to participate in co-design workshops?
11. Do you have any views on representation in the co-design process?
12. Do you foresee a need for particular focus groups?
13. Are there proposed workshop topic/s which, in your view, might be missing or unnecessary?

Glossary

Access control: *Arrangements and systems to control physical access to facilities regulated under the* Aviation Transport Security Regulations 2005 *or the* Maritime Transport and Offshore Facilities Security Act 2005*.*

ASIC: Aviation Security Identification Card.

API: Application Programming Interface, which is a software intermediary that allows two applications to talk to each other.

ATSA: *Aviation Transport Security Act 2004.*

ATSR: *Aviation Transport Security Regulations 2005.*

AusCheck: The organisational unit in the Department of Home Affairs responsible for background checking services and administration, including the ASIC/MSIC issuing body of the Comptroller General of Customs.

AusCheck Advisory Group: The primary coordination body for providing advice in relation to AusCheck service levels and end user satisfaction, the security outcomes sought by the reform and the transition of existing issuing bodies out of the schemes.

AusCheck Core Capability Model: The business systems and processes being established by AusCheck to support transition to a single issuing body.

AusCheck Issuing Body: The business unit in AusCheck responsible for issuing body functions for the ASIC and MSIC schemes.

Co-design: A process of participative design as described in this paper.

Commercial issuing body: An issuing body which undertakes its activities on a commercial basis, and which is not otherwise regulated under the frameworks of the ATSA or MTOFSA.

Commercial partner: A commercial contractor to AusCheck, responsible for undertaking card production and distribution, and in-person identity verification, on behalf of the AusCheck Issuing Body.

Department: The Department of Home Affairs.

Employer: Employers and contract supervisors in facility operators, service operators and service providers whose engagement of workers creates a need for an ASIC or MSIC.

Facility operator: An entity which manages a transport facility that is regulated under frameworks of the ATSA or MTOFSA*.*

Future operating model: The operating model which is being developed to apply following transition.

Industry participant: A service operator, facility operator or service provider which is regulated under the frameworks of the ATSA or MTOFSA.

Industry Partner: A partner which is appointed by AusCheck to undertake in-person identity verification on behalf of the AusCheck Issuing Body.

Issuing Body: An entity appointed to be an issuing body under Division 6 of the ATSR or Division 6 of the MTOFSR.

Kinegram: A security identification card feature which is currently a requirement of the ASIC and MSIC schemes.

MSIC: Maritime Security Identification Card.

MTOFSA: *Maritime Transport and Offshore Facilities Security Act 2003.*

MTOFSR: *Maritime Transport Security and Offshore Facilities Regulations 2003.*

Remote/regional: Locations outside Australian capital cities.

Service provider: An entity that provides services to a facility operator or service operator, and whose staff require security identification clearances from AusCheck.

TAC: Temporary Aircrew Card.

Transition: The period during which issuing bodies are progressively transferring to AusCheck prior to the AusCheck Issuing Body being the single national issuing body.

VIC: Visitor Identification Card.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

AusCheck

Contact: IBReformProject@homeaffairs.gov.au

Web: www.auscheck.gov.au