CORPORATE GOVERNANCE

We maintain a strong culture of integrity and transparency, supported by a robust corporate governance framework. This framework comprises various policies that guide everyone in Capital A towards ethical behaviour when dealing with our stakeholders, reflecting our values and upholding our reputation.

Policies that guide the way we conduct our operations Group-wide

Policy	What It Is	Introduced/Last Updated
Code of Conduct	Guidelines that clearly outline the standards of ethics expected	2020
Anti-Bribery and Anti-Corruption Policy	Guidelines to prevent bribery and conflicts of interest, addressing: gifts & hospitality; dealings with partners, suppliers & public officials; political contributions; sponsorships & charitable donations; facilitation payments	2020
Whistleblowing Policy	Platform for Allstars and third parties to report any instance of unethical behaviour, while protecting whistle-blowers from reprisals	2018
Conflict of Interest Policy	Guidelines and procedures on situations such as receiving or offering gifts, with the objective of enabling accountability and transparency	2016
Non-disclosure and Confidentiality Policy	Guidelines to protect the Group's confidential and proprietary information	2018
Disciplinary Policy	Procedures to handle any breach of established norms/Code of Conduct	2021
Workplace Search Policy	Gives the company the right to conduct searches on Allstars to prevent misconduct	2008
Remuneration Policy	Provides clarity on remuneration structures and practices for Board of Directors and Allstars	2020
Board Diversity Policy	Guidance to achieve sufficiently broad representation on the Board for balanced and fair decision-making	2018
Anti-Harassment Policy	Provides guidelines on the establishment of in-house mechanisms to prevent and eliminate any forms of harassment involving the Allstars	2021

[For more information on our Corporate Governance, please refer to the Corporate Governance Overview Statement on pages 163 to 173]

Ethics & Integrity

All directors and employees at Capital A are expected to comply with the Group's Code of Conduct and Ethics (the Code). The Code addresses aspects such as confidentiality of information, conflicts of interest, money-laundering and/or insider trading/dealing, environment, health and safety and whistleblowing.

Developed by the Group's People Department, in November 2021 the Risk Management Department (RMD) was assigned to look at Group-wide compliance. Through a compliance exercise and matrix, RMD will develop a central compliance repository (internal & external) for better monitoring. To ensure effective communication on policies and procedures, all new hires are introduced to the Code during their onboarding sessions and are required to acknowledge the Code online. Moving forward, we aim to conduct refresher training on the Code and develop an e-learning module to reinforce a culture of integrity.

To ensure adherence to these policies, we encourage Allstars throughout the Group to speak up and report any incidents that go against the grain of the standards we seek to achieve. There are two main channels through which they can do this:

- askPAC System: a chatbot where they can raise concerns on unfair or discriminatory treatment, and every query will generate a serial number for easy tracking. All reports are directed to the Employee Relations team.
- Whistleblower channel: where Allstars and any other stakeholder can send emails in confidence via whistleblower@airasia.com, which is managed by our Internal Audit team. Concerns related to employment matters will be redirected to Employee Relations. For more information on our Whistleblowing channel, please refer to https://capitala.airasia.com/whistleblowing_channel.html.

Types & incidence of breach in ethical behaviour

Types of Breach	Total	Actions Taken
Harassment	2	Termination of Employment
Fraud	9	Warning, Final Warning, Termination of Employment
Misappropriation of company assets/funds	1	Warning
Abuse of company benefits/property	0	-
Others (eg breach of internal SOPs, attendance, late to work)	117	Warning, Final Warning, Termination of Employment

Whistleblowing Channel

In 2021, we received a total of 19 reports via our whistleblowing channel concerning abuse of authority/benefits (three reports); misappropriation of company assets/funds (one); and others (15). These cases were investigated and dealt appropriately with follow-up actions.

Anti-Bribery & Anti-Corruption (ABAC)

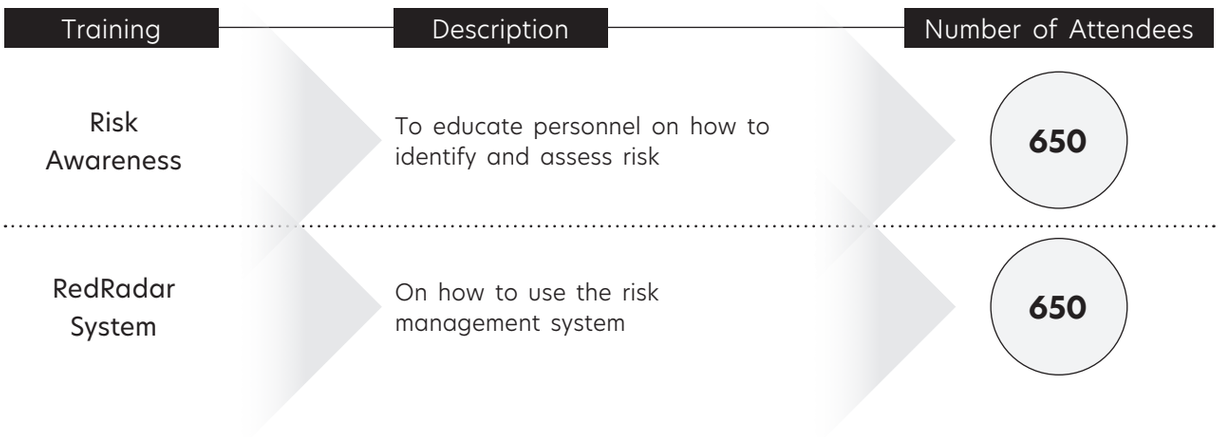
Capital A does not tolerate any form of bribery or corruption. When we revised our ABAC Policy in 2020, in response to Section 17A of the Malaysian Anti-Corruption Commision (MACC) Act 2009, we ensured all Allstars were aware of the Policy and the seriousness of a breach. Our ABAC Policy is available to all employees via the Group's intranet, RedDocs, and our official website.

Corruption has the potential to severely undermine our business, therefore RMD continuously monitors the Group for any potential corruption risk. In the last four years, two cases of bribery/corruption were proven. These were managed as per outlined procedures, with warning letters and dismissal, if warranted.

Risk Management

Over the last year, RMD has worked to transform what used to be a very theoretical approach to risk and business continuity management to one that is more practical and people-friendly. This has been achieved through updating and automating our risk and business continuity management using RedRadar, our risk management system. More interactive, the system now sends reminders to accountable personnel of due dates for risk assessments, complete with an escalation process that creates accountability should the risk assessment not be completed on time. To ensure the relevant people are able to use RedRadar optimally, training was provided to heads of department and stations as well as designated risk personnel. In addition, risk awareness training was provided to educate Allstars on what constitutes risk and how to assess risks. Our ultimate objective is to create a risk-aware culture that permeates our daily activities and functions.

Risk awareness training for employees



Four main risk categories are assessed on a quarterly basis: Financial, Operational, Strategic and Compliance Risks. Within these broad risk categories, emerging and long-term risks are identified and tracked.

Long-term risks identified

Category	Emerging Risks	Description	Impact	Mitigation Actions
Strategy	Regulatory Risk	Change in regulatory structure	Regulatory changes that could change the business strategy	Continuous monitoring of regulatory changes
Operational	Human Capital Risk	Succession planning and succession management	Business continuity	Identification of successors
Financial	Financial Risk	Financial sustainability	Business continuity	Financial analysis on any business decisions

Business Continuity Management

Business Continuity Management, which entails having a Business Continuity Plan (BCP), is a crucial component of our risk assessment as it involves the assessment of key functions – ie our people, processes and systems – utilising the Business Impact Analysis (BIA) framework. Through BIA, we are able to ascertain the severity, urgency and impact of any failure in the Group's function(s). Heads of all key function areas proactively review the BCP on a half-yearly basis.

In 2021, in response to extreme climate events in Thailand and the Philippines, we undertook BCP exercises at Bangkok's Don Mueang Airport and the Cebu, Puerto Princesa and Tacloban airports in the Philippines.

AirAsia Thailand Flood Scenario Readiness Simulation at Don Mueang (DMK) Airport, Bangkok

No.	Test Activity	Test Location	Departments	Test Date	Test Findings
1	Planned flood scenario readiness simulation	Don Mueang (DMK)	All Operations departments	12 October 2021	• All departments confident of the level of handling of the floods • Reactive approach is in line with the available response plan for diversion and mobilisation of aircraft/fleet
2	Unplanned Flight Operations mobilisation (recurrent from 2019 exercise)	Virtual meet (Google)	Flight Operations	21 December 2021	• Partial assets were unserviceable due to water damage • Ability to carry out operations as per business-as-usual with remaining equipment • No adverse impact on operations as rostering covered work from home during the event

AirAsia Philippines Business Continuity Activation during Typhoon Rai (Odette)

On 18 December 2021, the BCP was activated for Cebu (CEB), Puerto Princesa (PPS) and Tacloban (TAC) stations in response to Typhoon Rai. The cities of Cebu and Tacloban were severely impacted, experiencing loss of telecommunications infrastructure and disruption of electricity and water supply in many areas. However, the airports were still accessible and powered by generators, enabling the teams to access internet and communications infrastructure to operate flight-related systems. No AirAsia aircraft was stranded or based in these stations at the time of the incident, and no major equipment damage was reported.

While we continued situational monitoring, our teams in Manila loaded essential supplies such as food and sanitation items for affected Allstars on our first flight into Cebu after the typhoon.

Distribution of essential items to Allstars as flights resume at PPS airport

Test Activity	Impacted Locations	Departments	Date	Outcome/Results
BCP activation – Natural Disaster: Typhoon	Cebu (CEB), Puerto Princesa (PPS), Tacloban (TAC) Airports	Ground Operations Flight Operations Cargo Communications	18 December 2021	BCP was activated in tandem with transportation of essential supplies to Cebu
			27 December 2021	All staff accounted for and reported safe Business-as-usual restored in Cebu for arrival and departure flights including mobilisation of reservists
			11 January 2022	Stand down of PAA Red Code

Following a review of the BCP activation, it was determined that satellite phones and generator sets should be provided to all Philippines stations that are susceptible to prolonged power cuts and telecommunications disruptions due to natural or climate-related disasters.

GUEST EXPERIENCE

Despite severe disruption to air travel during the year, we continued to be guest-obsessed and ensured that all guests who flew AirAsia had the best possible experience from the time they booked their flights until they left the aircraft at their destination.

The happiness of our guests is the sole function of our Customer Happiness (CH) Team. The team, which has been ISO 1002:2018 (Customer Satisfaction, guidelines for complaints handling)-certified, has access to an Empowerment Matrix that helps them resolve issues and complaints as these are reported.

In 2021, we transitioned 95% of our CH Allstars to working from home. For our team's own happiness and well-being, daily huddle calls were organised while team leaders actively monitored work and rest hours to ensure a healthy work-life balance. In addition, starting 2020, all Allstars, including CH team members have access to our internal peer support team for assistance. Allstars requiring support may reach out anonymously via our EkoChilli platform and a peer supporter will respond via their preferred communications channel within 24 hours.

Communication with Guests

The CH team oversees all inbound customer support through multiple online channels: website, airasia Super App, social media (Twitter, Facebook and Instagram) and messaging (WeChat, WhatsApp and Messenger) platforms.

During the year, two new services were added to further enhance our communication efficacy:

Flight disruption automation

Guests are now notified instantly of any flight cancellation or schedule changes via SMS and emails.

Instagram messaging

Our chatbot AVA was introduced to Instagram Direct Message to reply instantly to guests. Previously, the process was managed manually by our agents.

Moving forward, we will enhance My Bookings to present a simplified self-service platform enabling guests to amend details of their flights. We also plan to introduce more inbound customer contact channels such as AirAsia Chat and voicebot for greater customer choice.

Enhanced Guest Services

For a better contactless customer experience, the following initiatives have been implemented:

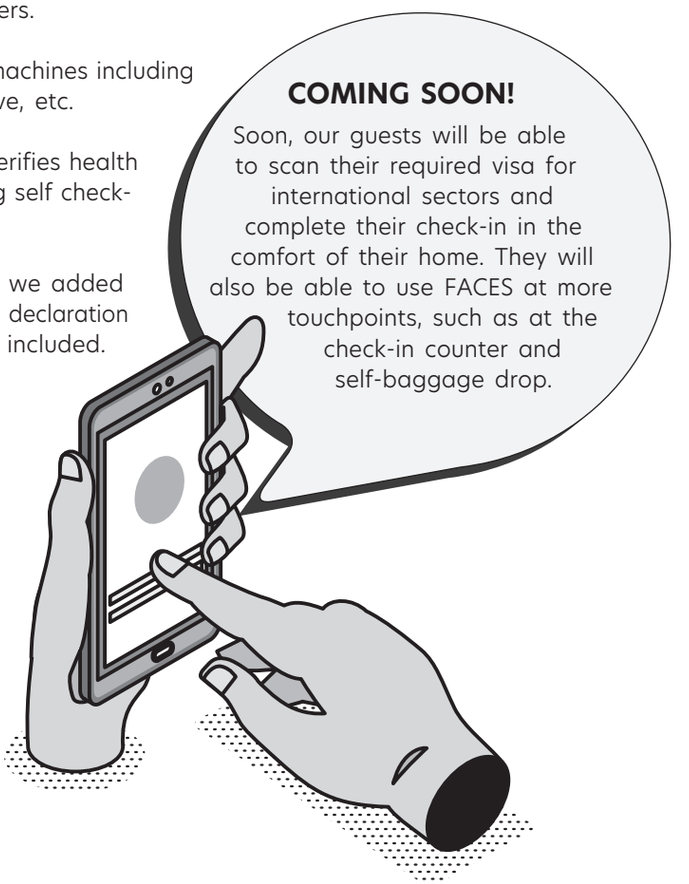
FACES: This first-of-its-kind in the commercial airline world facial recognition technology provides a contactless and seamless experience to guests at all touchpoints in their journey.

Galaxy Suite: This new platform hosts multiple systems that are required for Ground Operations functions such as check-in and FACES identification verification. AirAsia Guest Services staff at all 16 Malaysian airports are now able to assist guests to check-in and verify their documents using the app on their mobile devices without requiring guests to be physically present at a check-in counter. This enables us to deploy additional staff to quickly address long queues and check-in bottlenecks without having to open additional counters.

Contactless Payment: We introduced electronic data capture (EDC) machines including tap2phone to enable guests to pay securely via eWallets, payWave, etc.

Health Travel Pass (HTP): To facilitate travel during Covid-19, HTP verifies health documents such as vaccination certificates and RT PCR results during self check-in (both mobile and web).

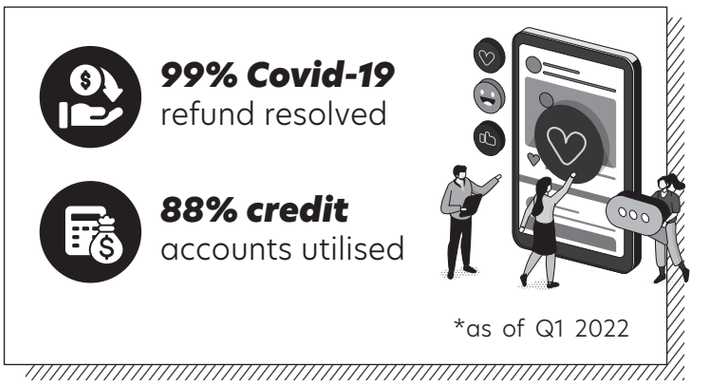
airasia Super App: For a faster and smoother check-in experience, we added a quick search function for passenger name record (PNR), online health declaration and new boarding passes. A download and share option was also included.



Net Promoter Score (NPS)

We have been monitoring our NPS since 2017. Emails are sent to guests before and after their trips for feedback on both their booking and flying experience with AirAsia. Their feedback informs us of how happy they are with our service and how likely they are to recommend AirAsia to others. The index ranges from -100 to +100, minus scores indicating that customers would not recommend the company.

Our NPS has risen significantly from 2017 to 2021, indicating positive and effective outcomes of efforts to ensure our guests are happy throughout their journey with AirAsia. As we have exceeded our target NPS scores for two years in a row, we are raising our target from 2022 onwards to 60 and above.



Year	NPS Score	Target
2017	17	NA
2018	31	NA
2019	38	NA
2020	52	50
2021	**60**	**50**

Awards

Awards validate our efforts to give the best value and experience to our guests all the time. In 2021, we continued to receive local and global recognition from well-known industry monitors. Awards during the year included:

On-Time Performance (OTP)

Key to keeping our guests happy as repeat customers is to ensure that our flights take off on time. Our OTP performance is closely monitored using digital tools and management walkabouts. Among the technologies implemented are an analytical toolset that provides greater visibility of OTP factors and other supplementary metrics that affect performance. Our team also applies a delay prediction algorithm to map out potential delays up to four hours in advance.

This early notification adds a buffer allowing our Operations teams to apply solutions that help mitigate and minimise the impact of delays. It also enables our Customer Happiness team to notify guests in advance so they are able to adjust their travelling plans, while our Guest Services team adjusts manpower allocations to ensure check-in counters are adequately staffed.

To monitor performance, weekly and monthly OTP reviews are held by all our AOCs. To continuously improve our service, we set the Group's OTP target at 85%. Our OTP for the period between 2019 to 2021 is shown in the table below.

AirAsia Load Factor and On-Time Performance, 2019-2021

Indicators	Measure		
	2019	2020	2021
Load factor for short-haul (<6 hours) (%)	85%	75%	74%
Percentage of short-haul flights (<6 hours) with more than 15 minutes delay	22%	15%	20%
On-time performance (%)	78%	85%	80%

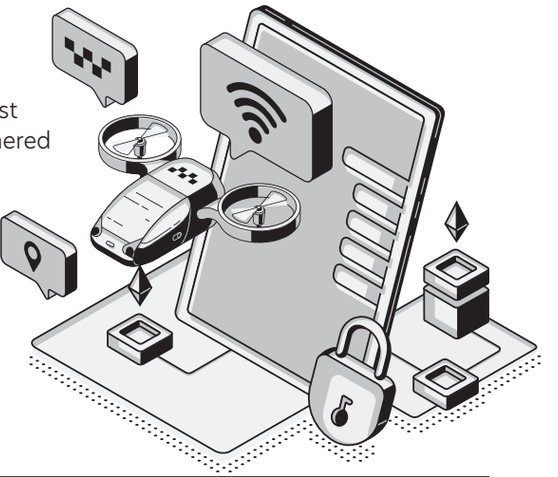
Between 2020 and 2021, we recorded a five percentage point increase in the number of delayed flights. This was mainly due to additional Covid-19 Customs, Immigration and Quarantine (CIQ) procedures that have been introduced by airports and health authorities. For example, Covid-19 regulations require that, after passengers disembark from an aircraft, the airline has to await the results of their Covid-19 tests before allowing new passengers to board. Should any passenger be symptomatic, the aircraft has to be thoroughly sanitised before on-boarding new passengers.

Another factor contributing to delays was the added complexity of managing a regularly changing set of Covid-19 regulatory rules which differ by country, and sometimes, states. These not only impacted check-in processes but also boarding times as Allstars have been requested to undertake additional documentation checks. While we do our utmost to communicate these new rules to Allstars and guests, the short notice given for implementation of new requirements resulted in lengthy delays in some cases.

However, we believe that there remains no immediate need to review our standard departure times as the changes are gradually being factored into our embarkation and disembarkation processes. In Indonesia, the streamlining of new policies and procedures has allowed us to recover our OTP performance by 40% compared to earlier in the year. Furthermore, many airports are easing requirements as Covid-19 enters into an endemic phase. We will continue to monitor our OTP and review our flight schedules on an ongoing basis.

TECHNOLOGY, INNOVATION & INFORMATION SECURITY

Technology & Innovation

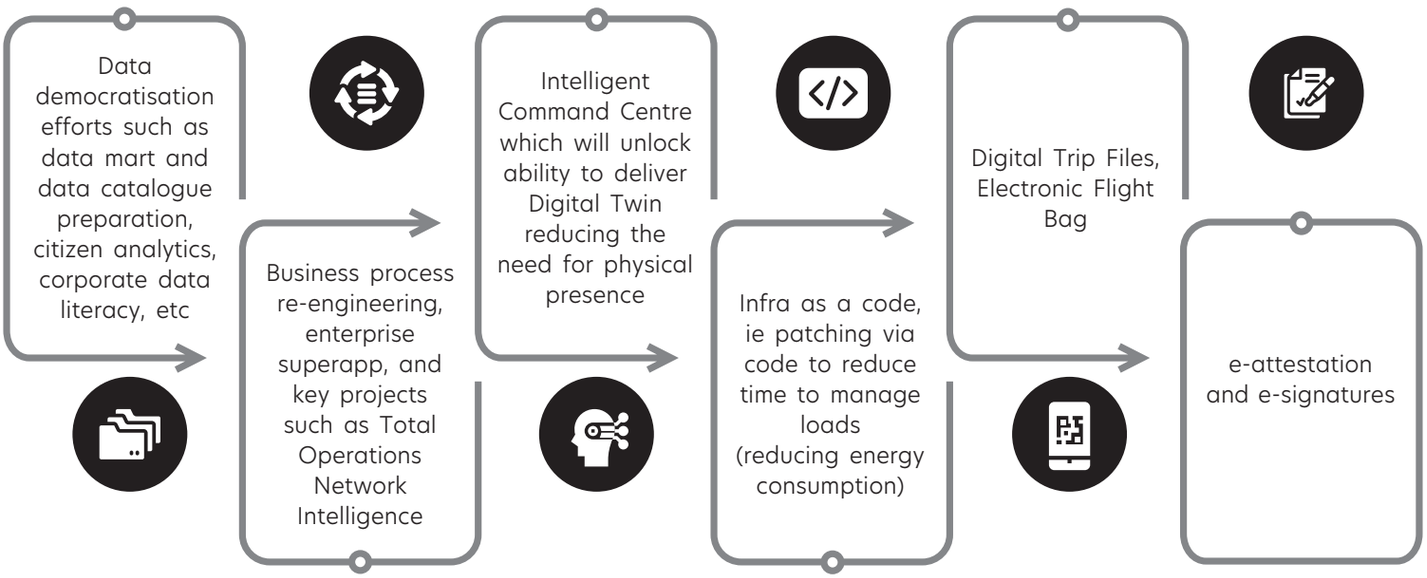


From the start, Capital A has been technology driven, leveraging technology to reduce costs and pass on the savings to guests. From an early adopter of online flight bookings to the present day, we have developed a sophisticated and robust digital infrastructure. This, together with the huge amount of data that we have gathered over the years, has enabled us to pivot to what we are today, namely a digital travel and lifestyle company.

Other than the Airlines, our core businesses comprise airasia Super App, Asia Digital Engineering, Teleport, BigPay and Ventures – all of which are either tech companies or tech-reliant companies. We continue to leverage our digital infrastructure and data to create and incubate more startups while expanding the products and services currently offered to meet customers' evolving expectations and needs.

Innovation	Description	Plans for 2022
Health Travel Pass	Standardised and secure mechanism to store and verify guests' health data, eg vaccination certificates and Covid-19 test results, to authenticate guests' health status before boarding them onto the plane. The pass was launched in Malaysia in September 2021, followed by Indonesia in October 2021.	Rollout in Thailand, Philippines, Korea, Macau, Taiwan, Cambodia and Vietnam
FACES	Biometric airport clearance solution that guests can use via airasia Super App to check in, conduct baggage drop, validate their identity and clear security – remotely. Guests can enrol for FACES on the Super App with registration open for all our AOCs using passports or national IDs. The pre-security clearance was piloted in klia2.	Continue to extend the use of FACES at more touchpoints in klia2 (eg from counters to transit and aerobridge) and roll out boarding and pre-security touchpoints at other Malaysian airports once the vendor transitions the solution to the cloud. Currently it is an on-premise solution (at klia2) and not scalable to other airports without incurring significant cost.
Network modernisation through virtualisation	Virtualisation is achieved using Software-Defined Wide Area Network (SDWan), which enables more efficient management of long-distance networks. SDWan makes it easier to utilise multiple connections to achieve higher network performance at lower cost. Overall benefits include network resilience, optimisation of equipment use and bandwidth as well as better fault tolerance. The network upgrade started in 2021 with our Sydney data centre.	Rollout in all Malaysian domestic airports.
Digital Trip Files	Digitalisation of documents that need to be filed by Ground Operations after a flight is completed in order to reduce paperwork and manual workflow on the ground.	The system will be updated with technical optimisation, monitoring and tracking enhancement, dashboard, trip records module in Galaxy Suite, and CAAM approval.

As we transition towards becoming a data-driven organisation, the following innovations will be introduced in 2022:

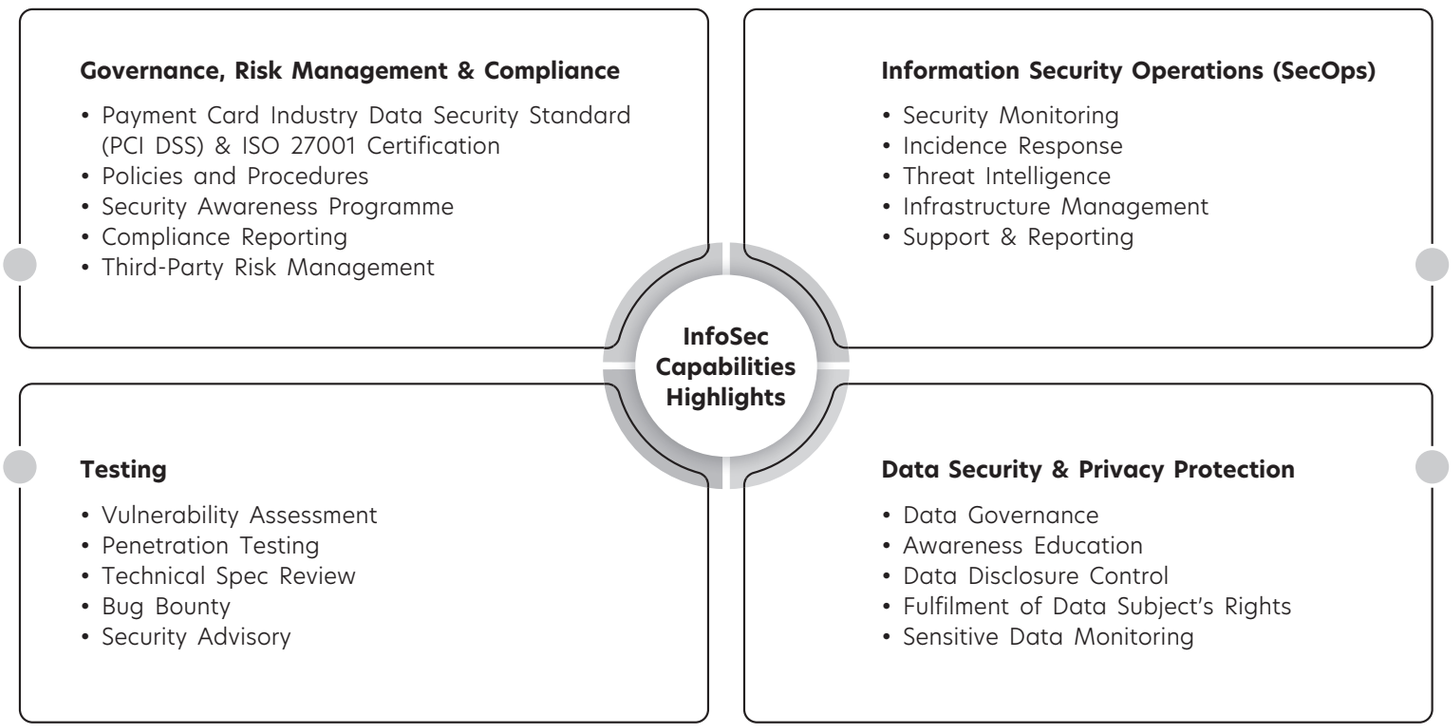


Information Security

The confidentiality and integrity of data and information are important to us. To further strengthen our governance practices, the Group Information Security has obtained its ISO 27001:2013 - Information Security Management certification in November 2021. By complying with ISO 27001, we are able to assure our stakeholders that their security assets such as financial information and personal details are safe.

To support our expansion in digital lines of business, we recognise that it is imperative to secure the information and data that are fundamental to our growth. The information security architecture of Capital A is built on four pillars covering governance, risk management and compliance (GLC), information security operations, testing as well as data security, and privacy protection.

The table below summarises the areas covered under these pillars.



As we are taking a new approach to information security disclosures, we will be covering this materiality area in more depth, discussing both existing frameworks and mechanisms, as well as new enhancements added in 2021.

(i) Governance, Risk Management & Compliance

Governance, Risk and Compliance (GRC) is the first pillar of the Group's information security capabilities. It refers to the alignment of policies and procedures with established standards, identification and mitigation of the Group's information security risks and compliance with relevant legal, regulatory and industry requirements.

Our information security governance structure is underpinned by the following policies which are reviewed annually in accordance with the requirements of ISO27001 certification:

Policy	Description	Changes in 2021
Information Security Policy	• Creates an environment that helps protect information resources and users from threats that could compromise privacy, productivity, reputation and intellectual property rights	• Updated Password and Anti-Virus Policies • Established Clean Desk and Clear Screen Policy to ensure sensitive/ confidential information are secured at all workspaces
Data Governance Policy	• Outlines how business activity monitoring should be carried out to ensure organisational data is accurate, consistent and protected • Defines the roles and responsibilities for information management • Specifies procedures to be used in managing different types of data	• Realigned with new Capital A organisation structure • Updated structure of data security & privacy workgroup

Policy	Description	Changes in 2021
Access Control Policy	• Outlines access controls across the Group's networks, information systems and services to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability • Protects the interests of all authorised users of the Group's information systems, as well as data provided by third parties, by creating a safe, secure and accessible environment in which to work	No major changes
Server, Database and Network Hardening SOPs	• Establish rules and procedures for hardening servers, database and network equipment to: a) create a security baseline for all servers, database and network equipment across the Group b) minimise server and IT-related risks c) comply with regulatory requirements	Increased frequency of re-hardening process
Information Security Incident Response	• Ensures operations recover quickly from information security incidents, minimising loss of information and disruption of services • Protects the Group's reputation and minimises loss of credibility among customers • Provides technical guidelines on responding to incidents effectively and efficiently	Updated Information Security Incident Response and Antivirus

In 2021, the above policies were also updated and aligned with Capital A's new objectives and goals. Periodic reviews were performed in critical policy areas such as access controls and re-hardening of critical servers.

To ensure that information security culture is practised at all levels, we developed an information security awareness programme for Allstars. The first mandatory training was launched in February 2020. In March 2021, an updated annual awareness training was made mandatory for all Allstars and training completion status was tracked with our HR systems with progress updated to management. The programme consists of an introduction to information security, management of information security as well as data management and handling. Allstars are also made aware of current information security threats, ways to avoid potential threats and steps that they should take in the event that external perpetrators succeed in penetrating the company's cyber security defences. Other than the initial training, reminder notices are regularly published on the company's internal communications channels.

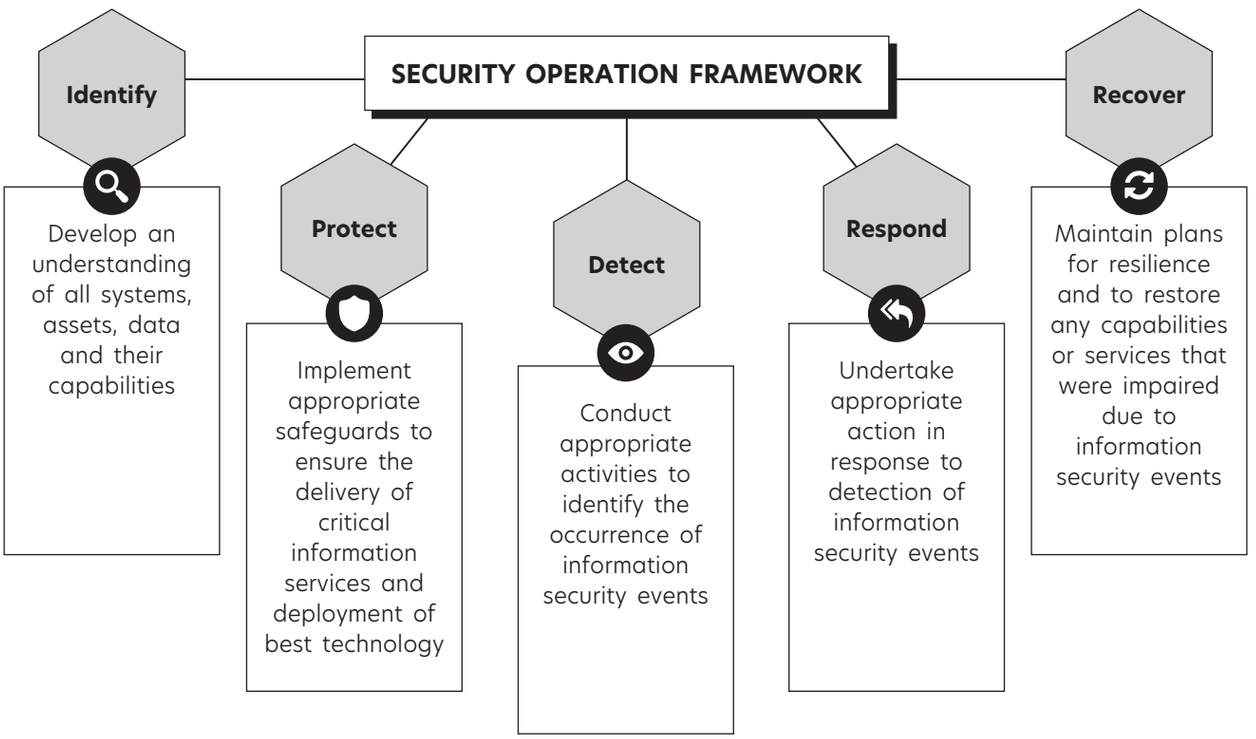
Capital A also practises a Report on Compliance (ROC) process to instil an information security culture within project management teams. The ROC's main objective is to ensure that information security aspects are taken into account in the commencement phase of a project's lifecycle. The ROC covers authentication and authorisation; management of data security and privacy; documentation of the technical specifications and implementation specifications; logs management and secure coding.

To meet industry standards, the GRC unit is further responsible for the annual renewal of the Group's Attestation of Compliance (AoC) certificate by our appointed Payment Card Industry Data Security Standard (PCI DSS) Qualified Security Assessor. For PCI DSS compliance, we are required to review and implement relevant policies and procedures, and conduct vulnerability assessments and penetration test lifecycles. On 26 November 2021, we obtained ISO 27001: Information Security Management System certification affirming our compliance with international standards on the management of information security. The certification is valid for three years with annual surveillance audits in between.

As Capital A's digital lines of business expand, we source a higher variety of technology-related services from third-party vendors. To manage our exposure to external risks, a third-party risk management process was developed to identify vendors that have access to the company's sensitive data or networks and perform due diligence on them to ascertain their resilience against threats. In 2021, we requested several vendors to provide additional audit requests for information (RFI) to demonstrate their compliance with our controls. These were adequately complied with.

(ii) Information Security Operations

The primary duty of Information Security Operations (SecOps) is to protect organisations against cyberattacks. To be effective, our cybersecurity architecture is organised in accordance with the US National Institute of Standards and Technology (NIST) Cybersecurity Framework which lays out five core functions of SecOps as illustrated in the diagram below. Each of these functions is performed concurrently and continuously to create an operational culture that addresses dynamic information security risk.



Our SecOps division is tasked with continuously monitoring and improving the Group's cybersecurity and information security position. The team holds a number of responsibilities including:

- Investigate potential incidents
- Triage and prioritise detected incidents
- Coordinate an incident response
- Monitor new and trending threats
- Identify and deploy solutions to new threats
- Address employee enquiries
- Report to management

With effective controls, our SecOps division has been able to prevent major cybersecurity attacks on our systems. No incidents were recorded in 2021.

Cybersecurity breaches and incidents

Indicators	2020	2021
Total number of information security breaches or other cybersecurity incidents	1	0
Total number of data breaches	1	0
Total number of customers and employees affected by company's data breach	1	0
Total value of fines/penalties paid in relation to information security breaches or other cybersecurity incidents (RM)	0	0

(iii) Information Security Testing

The main focus of Information Security Testing is to give assurance of the adequacy of security controls by coordinating security reviews through vulnerability assessment and penetration testing (VAPT) of the Group's IT infrastructure, network and web applications.

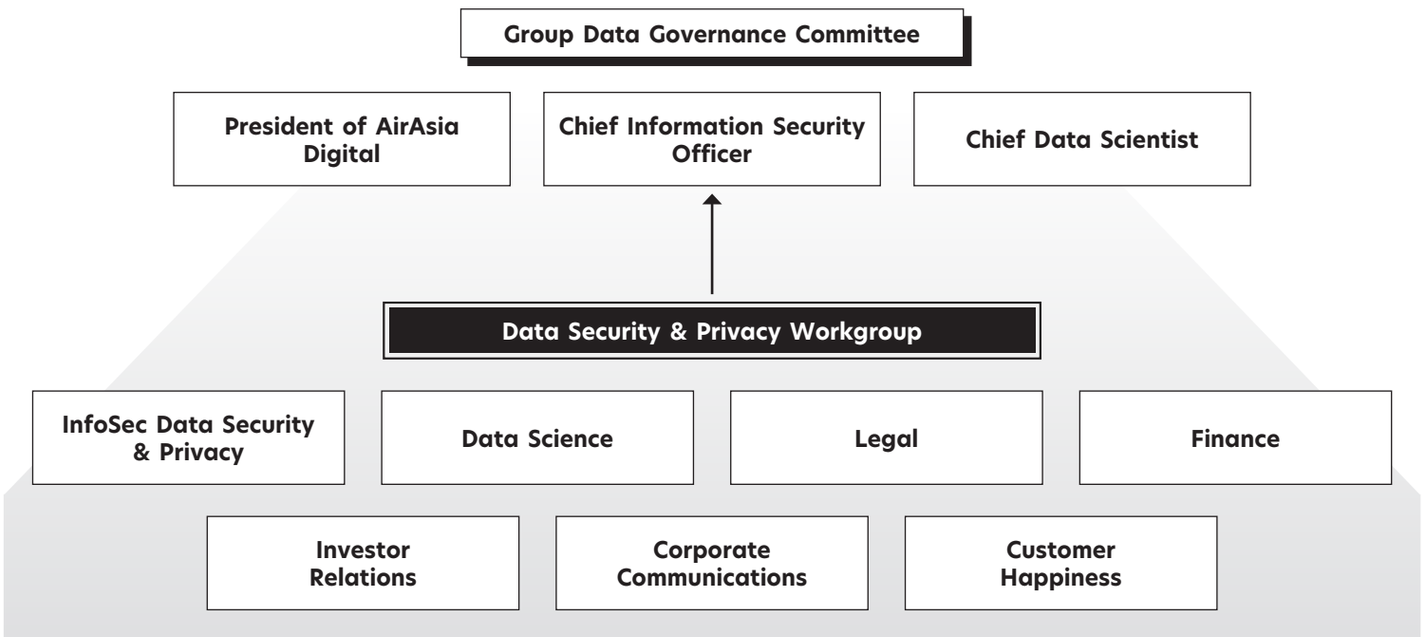
The VAPT approach allows us to have a more detailed view of the threats facing our applications. Below are some of the tools used by our team to find exploitable flaws and measure the severity of each finding.

Tool	Description
Ad hoc VAPT	VAPT represents two types of security testing which have different strengths and are often combined to achieve a more complete vulnerability analysis
Annual Vulnerability Assessment	Annual assessments to identify vulnerabilities in the Group's IT infrastructure, network and web applications
Source Code Review	Review of the software source code or API to find bugs and vulnerabilities
Technical Specification Document (TSD) Review	Review of documentation to ensure that technical specifications meet information security requirements, including the architecture, process flow, information security design and technologies used
Bug Bounty Programme	A platform for external security researchers to report vulnerabilities
Security Advisory	Notification to relevant teams for zero-day vulnerabilities, updates and software patches from software vendors

Our penetration testers are responsible for identifying vulnerabilities within the organisation's computing environment and for writing consumable VAPT reports. These reports are sent to the respective system or application owner for remediation. The team is also responsible for tracking the remediation progress and providing security consultation on the use of technology in meeting information security requirements.

(iv) Data Security and Privacy Protection

Capital A is committed to respecting and protecting the privacy of our customers, employees and third parties. We are equally committed to ensuring the confidentiality of information essential to our business.



Security of our internal data is assured through our Group Data Governance Policy. To govern the implementation of the policy, we established a Data Governance Committee, which is supported by the Data Security & Privacy Workgroup who meets regularly to provide advisory on data governance and review External Data Disclosure requests.

To meet the objectives of this division, we established a data classification framework to identify sensitivity levels of data and types of data indicating their origin and usage. All Allstars are made aware of our data governance processes through annual training coordinated by the Information Security division.

As Capital A now operates in a cloud environment, we raised the level of controls for sharing sensitive data in company emails and in document storage. In 2021, we added a data classification requirement on all cloud documents. Default sharing preferences were also changed to the least permissive option and a confirmation prompter added for extraneous sharing. We also scan all emails and documents for unmasked credit card numbers. If detected, the owners are notified of non-compliance for corrective action to be undertaken immediately.

Further, to control access to data, a Data Access Approval System was created and integrated with our IT Service Desk platform so as to automate the process to review and approve requests to access data belonging to the Group. This ensures that the applicant secures all levels of approvals before requested data is released.

Other than protecting our internal data, it is equally important for us to protect the privacy of our guests. In 2019, we issued our Personal Data Protection Standards Operating Procedures to ensure compliance with the Personal Data Protection Act 2010 of Malaysia. The SOP was updated in April 2021 to cover requirements under the electronic Information Law No. 19 of 2016 of Indonesia, Data Privacy Act 2012 of the Philippines and Personal Data Protection Act 2019 of Thailand.

At the same time, we empower our guests to manage their own data. In collaboration with the Customer Happiness and Communications departments, we enhanced FAQ articles available to our guests so that they are able to make corrections and updates. Our Customer Happiness agents were also trained to guide customers on channels to access their editable data.

SUPPLY CHAIN MANAGEMENT

We rely on a wide range of suppliers to help fulfil the needs of our diverse businesses. Recognising our ability to influence our suppliers, we seek to encourage sound ESG practices across our supplier chain. At the same time, we uphold the highest level of integrity and transparency in our dealings with suppliers as we build strong relationships based on trust.

To support the local economy, our preference is to source locally as far as possible. However, we also take into consideration user specifications, quality and compliance requirements, supply chain dynamics and other commercial issues in our vendor selection process.

Potential suppliers are invited to participate in a Request for Quotation or Proposal, following which their submissions are evaluated based on their ability to meet our specifications, target price, the quantity and quality of products to be supplied, delivery location and other operational/commercial requirements. Under certain circumstances we also assess the suppliers' financial health.

The recommended supplier is then presented to the relevant procurement approvers and stakeholders for review and approval. Thereafter, a contract may be put in place for clarity of responsibilities and accountabilities for both Capital A and the supplier, with the support of our Legal Team. Critical suppliers, as determined by Group Procurement, undergo an annual assessment to ensure they continuously improve the quality of the goods and services provided while keeping costs low. It is also an annual check-and-balance to ensure that suppliers understand and meet our risk and compliance policies.

Types of suppliers we engage with:

ICT	Food & Beverage (Inflight Food)	Facilities, Transportation, Logistics, Ground Service Equipment (GSE)	Commercial & Marketing	Professional & Facilities Services	General Items, Apparel & Merchandise
Critical suppliers (specialised and difficult to substitute)	Critical suppliers which are difficult to substitute due to stringent requirements of regulatory bodies. Certain suppliers, eg for water can be substituted	Choice of suppliers can be quite wide, subject to user requirements	Event suppliers are wide but choice of media agency is very selective based on commercial needs	Professional services suppliers are mostly specialised, however facilities services are mostly from local suppliers which come from a wider pool	Common pool of suppliers

Indicators	2019	2020	2021
No. of local suppliers excluding fuel, aircraft purchase & lessors	3,860	1,779	895
% spend on local suppliers	35	38	38
Total spend on local suppliers (RM)	RM622,002,369	RM572,184,262	RM575,651

We have a Supplier Code of Conduct (SCOC) which is communicated and mandated through our Terms & Conditions in our purchase orders (POs) and/or contracts. The SCOC covers:

- Business integrity and conflicts of interest
- Labour practices
- Confidentiality and personal data protection
- Environmental, health and safety management
- Social responsibility
- Competitive pricing and terms
- Anti-bribery and anti-corruption (included in 2021)

Our contracts carry a legal language to mandate suppliers to comply with all applicable laws and regulations.