



Insig AI
Sustainability Report
2022

Table of Contents

INTRODUCTION	3
APPROACH TO SUSTAINABILITY	3
SUMMARY	3
OUR IMPACTS.....	3
OUR RISKS	3
MATERIALITY	3
OVERVIEW OF KEY ISSUES	4
DATA SECURITY AND PRIVACY	4
WORKFORCE	4
ENVIRONMENTAL RISK AND IMPACT	4
DATA SECURITY	5
DATA SECURITY.....	5
SYSTEMATIC RISKS FROM TECHNOLOGY DISRUPTIONS.....	5
ISO27001 PROCESS.....	5
RISK ASSESSMENT.....	5
STATUS	6
CYBER SECURITY.....	6
DATA PRIVACY	6
WORKFORCE	7
WORKFORCE WELLBEING	7
HEALTH AND SAFETY.....	7
DIVERSITY, INCLUSION AND EQUALITY	8
BULLYING AND HARASSMENT.....	8
ENVIRONMENTAL RISK AND IMPACT	9
CLIMATE CHANGE – INDIRECT GHG EMISSIONS	9
TRAVEL	9
DATA CENTRES	9
WATER – INDIRECT WATER CONSUMPTION.....	9
CORPORATE GOVERNANCE	10
APPENDIX A: SASB SOFTWARE AND IT SERVICES STANDARD (2018): SUSTAINABILITY DISCLOSURE TOPICS AND ACCOUNTING METRICS	11
APPENDIX B.I: INSIG AI AWS CARBON REPORT (1 APRIL 2021-31 MARCH 2022)	13
APPENDIX B.II: INSIG DATA (FORMERLY FDB SYSTEMS) AWS CARBON REPORT (1 APRIL 2021-31 MARCH 2022)	15

Introduction

This Report has been prepared internally and approved by the Board of Directors for publication in conjunction with the Annual Report and Accounts for the period 1 April 2021 to 31 March 2022.

Approach to Sustainability

Insig AI believes that businesses have a duty to behave sustainably and responsibly in a way that minimises harm, and benefits society and our planet.

One of Insig AI's main business areas is providing innovative software to support best practice Environment, Social and Governance (ESG) research and analysis.

When it comes to our own impacts and risks, we want to demonstrate leadership in this space for a company of our size and industry.

This is our first published Sustainability Report, following an internal assessment during the previous reporting year which has been reviewed and updated for this reporting period.

Summary

Our impacts

Insig AI's mission for the ESG Research Tool and bespoke consultancy services is to drive best practice, transparency and evidence-based decision making in the sustainable investment space. In this way, we believe that we are contributing a positive social and environmental impact through our products and services, R&D and innovation.

At the same time, no business can exist without some environmental footprint, and this report sets out how we have assessed and will seek to minimise our negative impacts.

Our risks

ESG is a risk-orientated framework for stakeholders to assess non-financial factors that can impact a business' sustainability and resilience. We have taken a view on priority factors from the materiality approach of the Sustainability Accounting Standards Board (SASB), combined with our own position on social responsibility and expertise on how to mitigate these risks.

Materiality

The SASB *Standards for Software and IT Services* provides a framework for reporting on priority and material ESG issues. Materiality refers to financially relevant issues that are reasonably likely to impact the financial condition or operating performance of a company and, thereby, are most important to investors.

A summary table of these standards is contained in Appendix A and accounting metrics are referenced in the report alongside the relevant disclosure.

Overview of key issues

Data security and privacy

Data security and data privacy are the highest material risks to the business. A critical incident can lead to the loss of confidential material and service disruptions, and ultimately compromise our ability to deliver to our clients.

Details of our Information Security Management System which exists to mitigate these risks are reported below.

Workforce

Our skilled workforce and the intellectual property (IP) we hold are fundamental to the success of Insig AI, and loss of these is identified as a risk.

A healthy working environment, fair pay and diversity are built into our culture and these factors also enable us to attract and retain the best talent.

We report on our HR policies and procedures below and publish a certain number of these on our website.

Environmental risk and impact

As a small, hybrid-working company that uses renewables-based cloud computing for software development, we assess that our direct environmental impact and risk are relatively low.

We report an estimate of our main indirect carbon emissions below and in Appendix B and consider how to further manage this in the future.

Corporate Governance

We believe strong corporate governance is fundamental to the long-term success of all businesses and we hold ourselves to high standards.

Insig AI follows the 2018 QCA Corporate Governance Code and other relevant policies such as on anti-bribery and whistleblowing are detailed below and on our website.

The following section provides detail on the key risks and impacts we have identified and how these are being managed and mitigated.

Data Security

Information Security Management System

Insig AI has an approach to ISMS (Information Security Management System) which supports the governance and oversight of critical incident risk management as well as systemic risk management for both data privacy and cyber security.

Data security

The Information Security Officer is nominated and required to report any data security breach to the CEO. During the reporting period, there were no data breaches (TC-SI-230a.1).

As part of Insig AI's approach to identifying and addressing data security risks, all policies and procedures are documented and available online for all staff, including:

- Breach and Incident Reporting Policy
- Data Breaches – What do I need to know?
- General Data Protection Policy

Systematic risks from technology disruptions

Insig AI did not experience a performance incident or downtime issue that had a material impact on the business that required regulatory reporting to authorities or incurred financial penalties (TC-SI-550a.1).

The nature of Insig AI's business reduces the importance and prioritisation of proactive business continuity measures. Our business continuity program is based on cloud-based technology and the regeneration of environments using automated DevOps processes (TC-SI-550a.2).

ISO27001 process

We use the ISO27001 management system to embed information security in the organisation. Our ISO implementation was independently audited in October 2021. A decision has been made that as certification is not a business-critical priority, we are not performing monthly checks (TC-SI-230a.2).

The ISO process is implemented as follows:

1. Agree roles & responsibilities of the project team (CTO, Project Manager, DevOps Manager)
2. Assign the Security Officer role
3. Build a plan - do - check - act project based on industry best practice
4. Create 16 policies & 14 procedures
5. Perform security risk assessment across 36 potential risk areas
6. Annual Risk treatment plan

Risk assessment

The ISO process involves a risk assessment, in which 37 potential risk areas are analysed for exposure, as a combination of likelihood and impact.

A risk assessment was conducted in July 2021 - we identified 1 medium exposure risk and 1 high exposure risk.

Risks identified as 'high'	Description	Mitigation to 'low'
Leak confidential information during testing or demo	A salesperson uses a live production environment of another customer/an engineer uses production data to simulate an error on dev/test/acceptation environment	For software demos, a client-agnostic data set of global companies has been developed for use by both engineers, prospect demos and trials

Status

The 2021 annual risk assessment was performed on the PI Product team. We have reduced the number of high risks from 4 to 1 and medium risks from 6 to 1 by implementing appropriate measures.

We have subsequently acquired FDB Systems and the risk assessment needs to be performed on this part of the business.

Cyber security

All developers attend secure coding courses to ensure they are aware of best practices around securing our apps. All staff are made aware of secure behaviour around password policies, two factor authentication, data sharing and other high risk activities via internal training.

We use DevOps best practices to secure all infrastructure, and to limit access to it on an as-needed basis. Our on-boarding and off-boarding processes are strictly enforced and automated as far as possible.

Data privacy

Upholding the highest standards of client and staff data privacy is core to our business, recognising that this is our duty and would present a risk to our operations and reputation if not upheld.

Insig AI does not use any of its users' data for secondary purposes (SASB TC-SI-220.a.2) and has not had any incidents or legal proceedings associated with data privacy in the reporting period, or previously (SASB TC-SI-220a.3).

Insig AI has had no law enforcement requests for user information (SASB TC-SI-220a.4) and none of our products or services are used in countries subject to government censoring (SASB TC-SI-220a.5).

Regarding staff data privacy, policies are made available to staff including:

- Retention and Destruction Policy
- Privacy Notice for Staff

Workforce

As innovators in software development, Insig AI depends on the skilled technical and intellectual property of its staff, and their wellbeing and retention are a priority.

Insig AI makes over 20 workforce policies available internally for staff including:

- Absence Due to Illness and Injury Policy
- Adoption Policy
- Bullying and Harassment Policy
- Compassionate Leave Policy
- Disciplinary Policy
- Equal Opportunity Policy
- Flexible Working Policy
- Grievance Policy
- Health and Safety Policy
- Maternity Policy
- Parental Leave Policy
- Paternity Leave Policy
- Social Media Policy
- Social Media Use – Guidelines
- Time Off for Adoption Appointments Policy
- Time Off for Antenatal Appointments Policy
- Time Off for Dependants Policy

We also make public a selection on our website as detailed below.

Workforce wellbeing

Insig AI offers private healthcare to its staff and is committed to supporting a balanced and healthy lifestyle through social measures, for example, a channel to track and share exercise activities. Wellbeing check-ins are conducted twice a year by Human Resources with each member of staff.

Working practices have changed due to COVID-19 meaning that staff are now predominantly working remotely, with access to a shared office space for hybrid working. Insig AI plans to continue in line with its Flexible Working Policy for the foreseeable future and believes it brings work-life balance benefits.

Health and Safety

The Health and Safety of staff and anyone visiting our premises or affected by our work is the responsibility of the CEO.

Insig AI's Health and Safety Policy can be found in the *Results and Reports* section of our website [here](#).

Diversity, inclusion and equality

Insig AI believes in supporting the pipeline of talent and opportunity, regardless of skin colour, gender or background. We wholeheartedly support the principles of equal opportunity in employment and are opposed to all forms of unfair or unlawful discrimination.

We will treat all job applicants, employees, customers/clients, contractors and suppliers in the same way, regardless of any protected characteristic (age, disability, gender reassignment, marital or civil partnership status, pregnancy or maternity, race (including nationality, ethnic or national origin), religion or philosophical belief, sex or sexual orientation).

We believe that everyone has the right to be treated fairly and with dignity and respect at work, and to work without fear of discrimination, bullying or harassment. We employ a staff of multiple nationalities and pride ourselves on that diversity, recognising that individuals from a wide range of backgrounds can contribute a wealth of experience to achieving our objectives.

The number of women at different levels of the business is as follows, full time employees only (TC-SI.330a.3):

Board: 0 (0%)

Management (Head of Dept): 2 (29%)

Skilled technical: 5 (33%)

We don't currently report on racial/ethnic group representation, employee engagement and foreign nationals including those located offshore, and will endeavour to do so in the next reporting period.

Insig AI's Equal Opportunity Policy can be found in the *Results and Reports* section of our website [here](#).

Bullying and harassment

We believe that all our employees, contractors and workers have the right to work in an environment free from bullying behaviour and any form of harassment, whether this is on the grounds of a protected characteristic (age, disability, gender reassignment, marital or civil partnership status, pregnancy or maternity, race (including nationality, ethnic or national origin), religion or philosophical belief, sex, sexual orientation) or indeed any other characteristic such as appearance, regional dialect or political stance.

Such behaviour will not be tolerated, and we seek to ensure that our working environment is sympathetic to everyone with whom we deal with in our working activities and that they are treated with dignity and respect.

Following COVID-19 and the shift towards remote working, a Slack Etiquette Policy was also made available to staff.

Insig AI's Bullying and Harassment Policy can be found in the *Results and Reports* section of our website [here](#).

Environmental Risk and Impact

Insig AI is a remote-working company which leases a minimal office space. We assess that our direct environmental risks and impacts around climate change, the water environment, waste generation and biodiversity are not currently material.

We report in line with the SASB framework below regarding our indirect Greenhouse Gas (GhG) emissions and will seek to report on water-related information in the future.

Climate change – indirect GhG emissions

Travel

Several members of staff live abroad and work remotely with minimal requirement for travel. Internal and external meetings are conducted virtually wherever possible and international travel is kept to a minimum.

Certain management staff take international flights regularly as required for in-person meetings. Their combined annual carbon footprint is estimated to be a total of 27 tCO₂e per year. This calculation has been done using www.myclimate.org. Greenhouse gas emissions are commonly measured in metric tonnes (MT) of Carbon Dioxide equivalent - MTCO₂e or tCO₂e.

Carbon offsetting is considered a last resort once emissions have been reduced as much as possible by other means. We are considering whether to engage in a high-quality carbon offsetting programme for emissions associated with unavoidable international travel.

Data centres

There is an energy demand associated with cloud computing data storage centres from 3rd party providers. Insig AI's main data provider is Amazon Web Services (AWS).

AWS provide a carbon emissions report, which estimates that Insig AI's total emissions for the period was 0.3 tCO₂e. The data centres used by Insig AI use either total or predominantly renewable power. The AWS emissions reports for Insig AI and Insig Data can be found in Appendix B (TC-SI-130a.1)

We are exploring the feasibility of locating all our data centres in regions that are 100% renewable and switching to more energy efficient servers provided by AWS (TC-SI-130a.3).

Water – indirect water consumption

We do not currently have water consumption and water stress data for our AWS servers and will seek to request this from AWS for future disclosure in line with the SASB accounting metrics.

Corporate Governance

Insig AI adheres to the 2018 QCA Corporate Governance Code, and our Statement of Compliance can be found online [here](#).

The following documents are shared internally with staff, some of which can also be found in the *Results and Reports* section of our website [here](#).

- Whistleblowing Policy
- Business Ethics and Integrity Policy
- Anti-Bribery and Corruption Policy
- Criminal Finances Act Policy
- Market Abuse (Insider Trading) Policy

Appendix A: SASB Software and IT Services Standard (2018): Sustainability Disclosure Topics and Accounting Metrics

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-SI-130a.1
	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Quantitative	Thousand cubic meters (m ³), Percentage (%)	TC-SI-130a.2
	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	n/a	TC-SI-130a.3
Data Privacy & Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	n/a	TC-SI-220a.1
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with user privacy ²	Quantitative	Reporting currency	TC-SI-220a.3
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-SI-220a.4
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring ³	Discussion and Analysis	n/a	TC-SI-220a.5
Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected ⁴	Quantitative	Number, Percentage (%)	TC-SI-230a.1
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-SI-230a.2
Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that are (1) foreign nationals and (2) located offshore ⁵	Quantitative	Percentage (%)	TC-SI-330a.1
	Employee engagement as a percentage ⁶	Quantitative	Percentage (%)	TC-SI-330a.2
	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees ⁷	Quantitative	Percentage (%)	TC-SI-330a.3

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Intellectual Property Protection & Competitive Behavior	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations ⁸	Quantitative	Reporting currency	TC-SI-520a.1
Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime ⁹	Quantitative	Number, Days	TC-SI-550a.1
	Description of business continuity risks related to disruptions of operations	Discussion and Analysis	n/a	TC-SI-550a.2

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
(1) Number of licenses or subscriptions, (2) percentage cloud-based	Quantitative	Number, Percentage (%)	TC-SI-000.A
(1) Data processing capacity, (2) percentage outsourced ¹⁰	Quantitative	See note	TC-SI-000.B
(1) Amount of data storage, (2) percentage outsourced ¹¹	Quantitative	Petabytes, Percentage (%)	TC-SI-000.C

Appendix B.I: Insig AI AWS Carbon Report (1 April 2021-31 March 2022)

Customer Carbon Footprint Tool

Apr 2021 - Apr 2022

Your carbon emissions summary Compares your carbon emissions with on-premises computing equivalents		
0.0 MTCO ₂ e Your estimated AWS emissions	2.2 MTCO ₂ e Your emissions saved on AWS	
Your emission savings		
2.2 MTCO ₂ e Saved from AWS renewable energy purchases	0.0 MTCO ₂ e Saved by using AWS computing services	
Your emissions by geography		
You don't have any carbon emissions for this time period.		
Your emissions by services		
Service	Carbon emissions	%
Total	0.0 MTCO₂e	100%

Your AWS carbon emission statistics

Month ▼

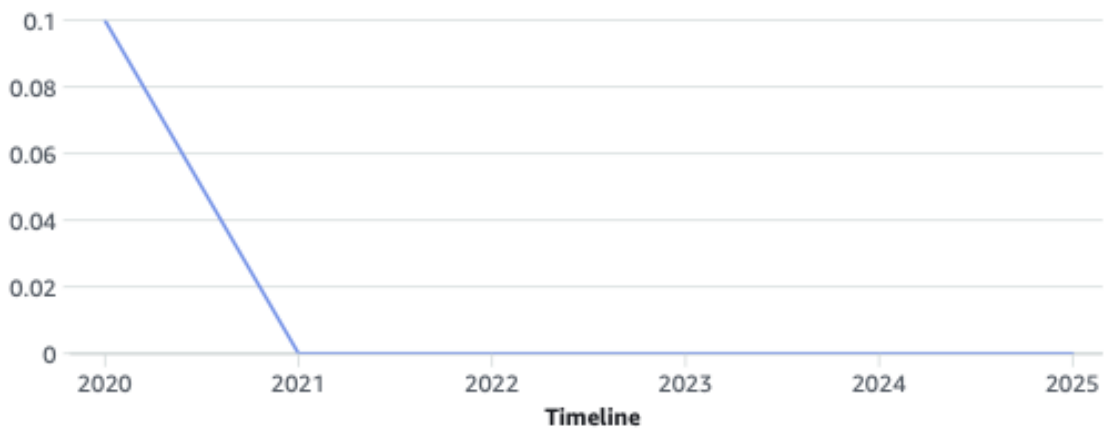
Carbon emissions (MTCO₂e)



Path to 100% renewable energy

Based on your current AWS usage, this chart represents projected changes in your yearly emissions as AWS works toward its goal of powering our operations with 100% renewable energy. Note: The date range you choose in the previous section doesn't impact the chart results.

Carbon emissions (MTCO₂e)



Appendix B.II: Insig Data (formerly FDB Systems) AWS Carbon Report (1 April 2021-31 March 2022)

Customer Carbon Footprint Tool

Apr 2021 - Apr 2022

Your carbon emissions summary

Compares your carbon emissions with on-premises computing equivalents

0.3 MTCO₂e

Your estimated AWS emissions

0.8 MTCO₂e

Your emissions saved on AWS

Your emission savings

0.6 MTCO₂e

Saved from AWS renewable energy purchases

0.2 MTCO₂e

Saved by using AWS computing services

Your emissions by geography



Your emissions by services

Service	Carbon emissions	%
---------	------------------	---

Service	Carbon emissions	%
EC2	0.1 MTCO2e	33.33%
S3	0.1 MTCO2e	33.33%
Other	0.1 MTCO2e	33.33%
Total	0.3 MTCO2e	100%

Your AWS carbon emission statistics

Month ▼

Carbon emissions (MTCO2e)



Path to 100% renewable energy

Based on your current AWS usage, this chart represents projected changes in your yearly emissions as AWS works toward its goal of powering our operations with 100% renewable energy. Note: The date range you choose in the previous section doesn't impact the chart results.

Carbon emissions (MTCO2e)

