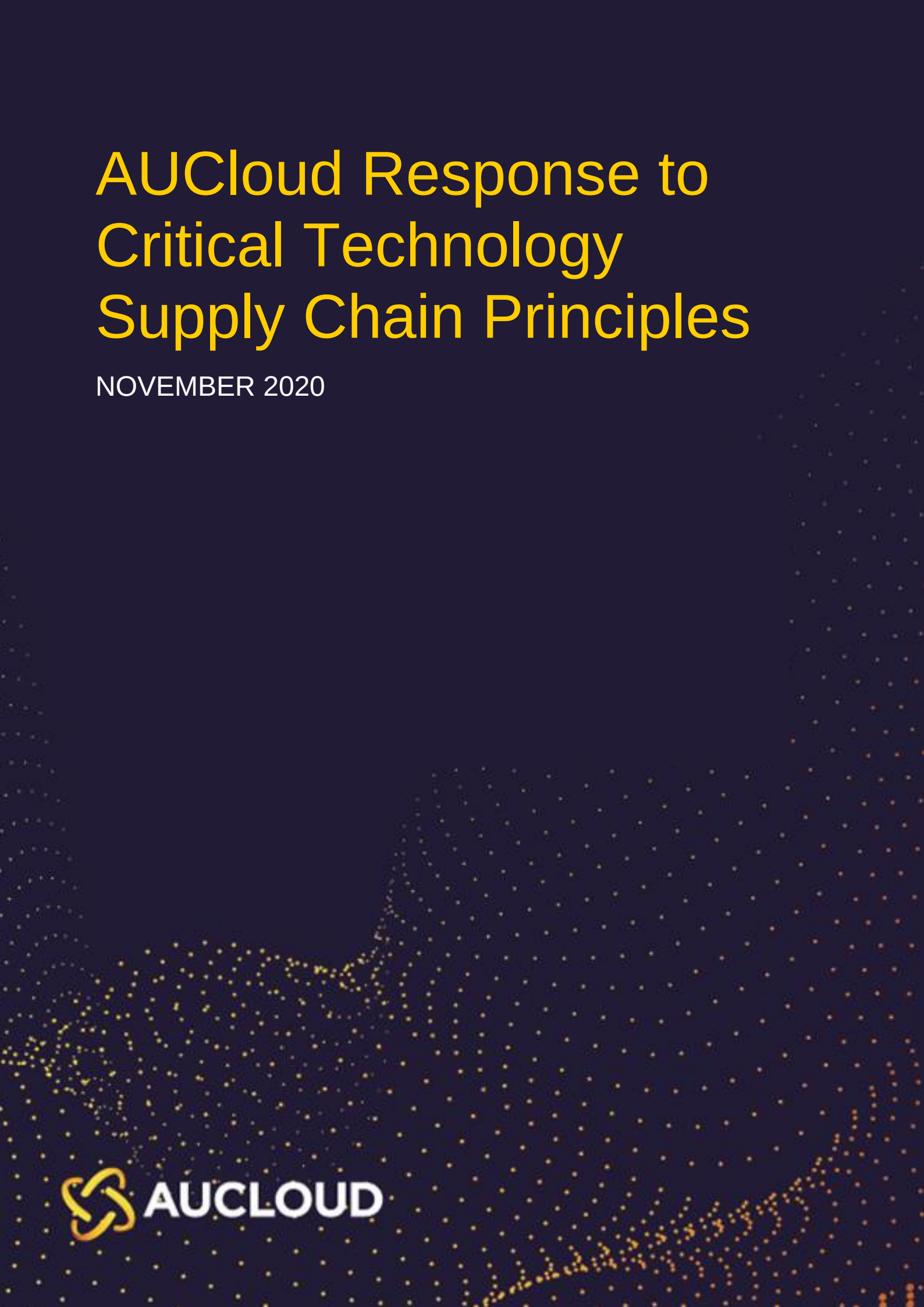
AUCloud Response to Critical Technology Supply Chain Principles

NOVEMBER 2020



Disclaimer

The information in this Proposal is the confidential information of Sovereign Cloud Australia Pty Ltd ("AUCloud"). Such information must confidential at all times and used solely to consider the Proposal put forth by AUCloud. You agree to take such measures to prevent the disclosure of the information as you would to prevent the disclosure of your own proprietary information, but in all cases, shall use at least reasonable care.

You do not acquire any rights in the information. All AUCloud trademarks and logos belong to Sovereign Cloud Australia Pty Ltd. Other trademarks and logos belong to their respective owners and are used for informational purposes only.

The contents of this document constitute valuable proprietary and confidential property of AUCloud and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorised in the applicable license agreement(s) pursuant to which such material has been furnished. In the event there are no applicable license agreement(s) governing the use of this material, please be advised that any use, dissemination, distribution, copying or disclosure of all or any part of this material not specifically authorised in writing by AUCloud in advance is strictly prohibited.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

Table of Contents

Introduction

Thank you for the opportunity to comment on the Critical Technology Supply Chain Principles. We hope you find our comment useful. Please do not hesitate to contact us if you require further details. Our comments are short but supportive of the Principles.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the needs of the Australian Government and Critical National Infrastructure (CNI) communities. This includes Federal, State and Local Governments and CNI organisations such as telecommunications, electricity, energy, financial services and similar utility providers.

Security is core to how we operate at AUCloud.

Independently IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM). AUCloud provides two independent environments: an Official Data Community Environment (ODCE) and a PROTECTED Data Community Environment (PDCE) that meet or exceed these controls based upon the August 2020 version of the ISM.

In addition, AUCloud's IaaS offerings and supporting business processes have also been certified against the International Standard for Information Security (ISO/IEC 27001).

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

AUCloud operates from two Data Centres: Sovereignty Zone 1 in Canberra and Sovereignty Zone 2 in Sydney, both designed to meet ASIO T4 standards for Zone 4 security.

Response

AUCloud supports the Principles as they stand and for the purpose of serving an advisory function to Australian technology businesses that rely on local, national and global supply chains for the hardware/software that enables their products and services. In our view they are, in any respect, good business practice for any cyber aware technology business.

AUCloud supports that the Principles should be voluntary.

As a sovereign cloud IaaS provider, we already align with the core themes of articulated in the Principles, ie., Security by Design, Transparency and Autonomy and Integrity. We effectively align with each of the 10 Principles.

The Principles are entirely consistent with work relating to the Critical Infrastructure Protection Bill, ASD's Cloud Security Assessment and Authorisation Guidelines and the Data Availability and Transparency Bill and Accreditation Framework. All include a strong focus on appropriate data management and protection. While further harmonization is required across documents (language, definitions), overall they share the same intent, notwithstanding their different purpose. They are consistent in terms of adopting a risk identification and mitigation position to strengthen Australia's overall sovereign resilience.

We note the 'sensitivity' related to Principle 8 regarding the influence of foreign governments on suppliers. The Principle is (as are all the Principles) advisory and aims to encourage businesses to appropriately identify and mitigate potential risks – something they should be doing anyway. It is also entirely consistent with the focus of the Cloud Assessment and Authorisation Framework which similarly identifies the need to consider extraterritorial risks and mitigate accordingly.