「Cloud Controls Matrixの全体像」

CSA Japan Congress 2024

一般社団法人　日本クラウドセキュリティアライアンス

理事　諸角昌宏

CSAリサーチフェロー、 CCSP、CCSK、CCAK、CCZT

2024年11月20日

プロフィール

- 一般社団法人日本クラウドセキュリティアライアンス　理事
- Cloud Security Alliance リサーチフェロー
- ISC2 Official Training Instructor
- CSA Authorized Instructor

本日のアジェンダ

1. CSA が提供する評価フレームワークCCM、CAIQ、CAIQ-Lite、STAR認証とは？
2. Cloud Controls Matrixの全体像
3. CCM関連情報へのリンク

1. CSA が提供する評価フレームワーク CCM、CAIQ、CAIQ-Lite、STAR認証とは？

CCM、CAIQ、CAIQ-Lite：　一言でいうと！

- **CCM（Cloud Control Matrix）**
  - CSAが提供するクラウドセキュリティ管理策集
  - 17ドメイン、197の管理策
- **CAIQ（Consensus Assessment Initiative Questionaire）**
  - CCMの各コントロールの内容をブレークダウンし、チェックリスト化
  - 質問数
    - 261個
- **CAIQ-Lite**
  - CAIQの縮小版
  - 以下の方針に基づく厳選された内容
    1. CSA本部において、CAIQ-Liteのさまざまなバージョンを考案し、メンバー間で共有し内部研究を実施
    2. クラウドサービスを評価する利用者からのフィードバックを入手
    3. 600人以上のITセキュリティ専門家による統計分析を行い、クラウドサービスの評価を行う際にCAIQのどの質問が最も適切かの判断を実施

CCM、CAIQ、CAIQ-Liteの利点（4つのポイント）

1. タダ（無料）

- 商用利用でない場合、無料で利用可能
- CSAのウエブサイトから自由にダウンロード可能
- 日本語版はCSAジャパンのウエブサイトから自由にダウンロード可能

2. グローバル

- グローバルに通用する。グローバルに同じ内容で提供
  （CCM V3.0.1やCAIQ V3.0.1は10か国語に翻訳提供）
- グローバルに展開している企業は、統一したセキュリティ基準で評価した内容を各国で提供可能

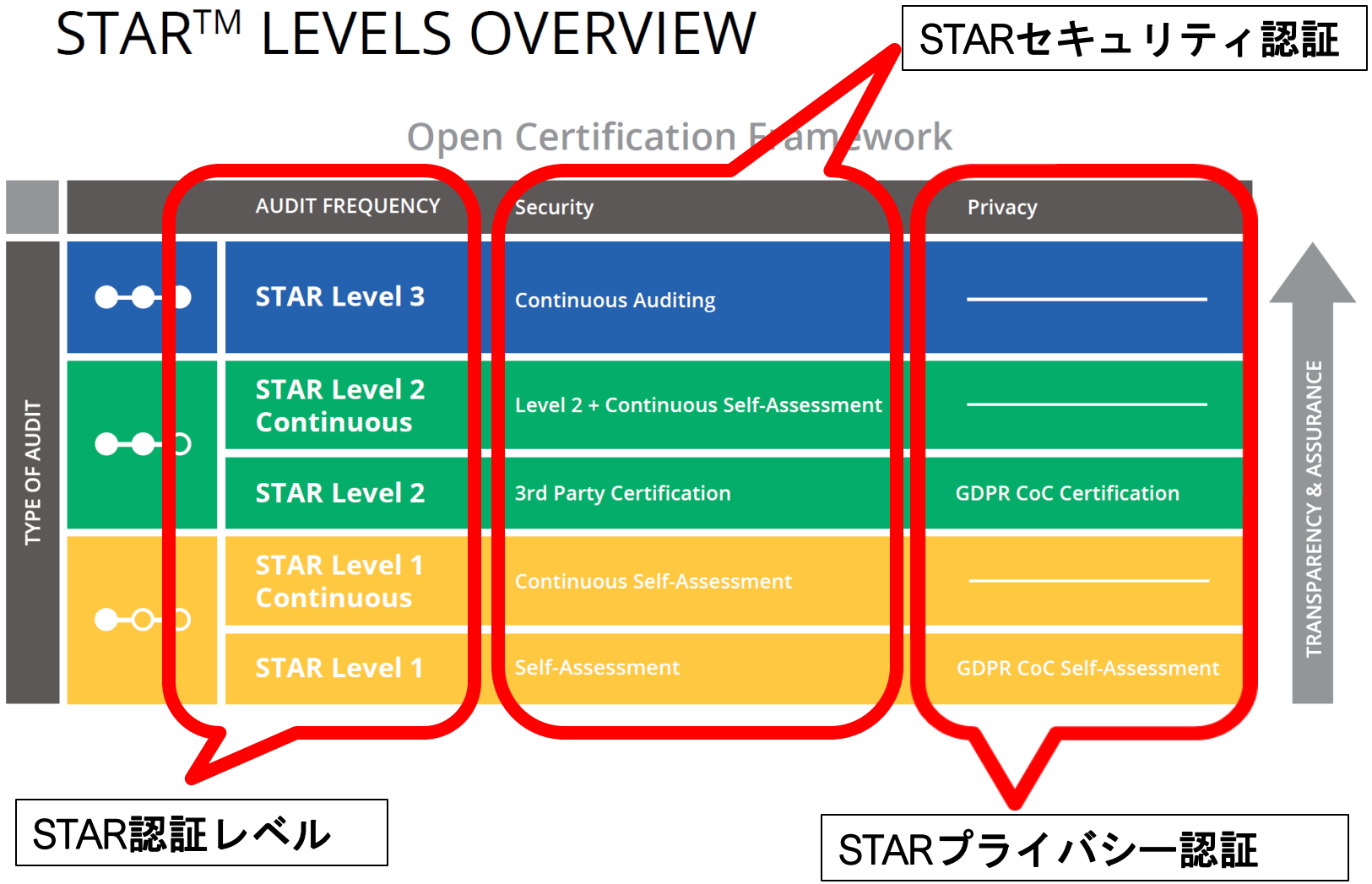
3. クラウドセキュリティに特化

- 提供されている管理策などは、すべてクラウドサービスおよび関連する技術
- チェックリストを作成する際、チェックリストの網羅性を高めることが可能

4. 透明性

- 自己評価結果を公開するサイト（STAR Registry）を用意。STAR Registryも無償で利用可能

STARプログラム　(1)

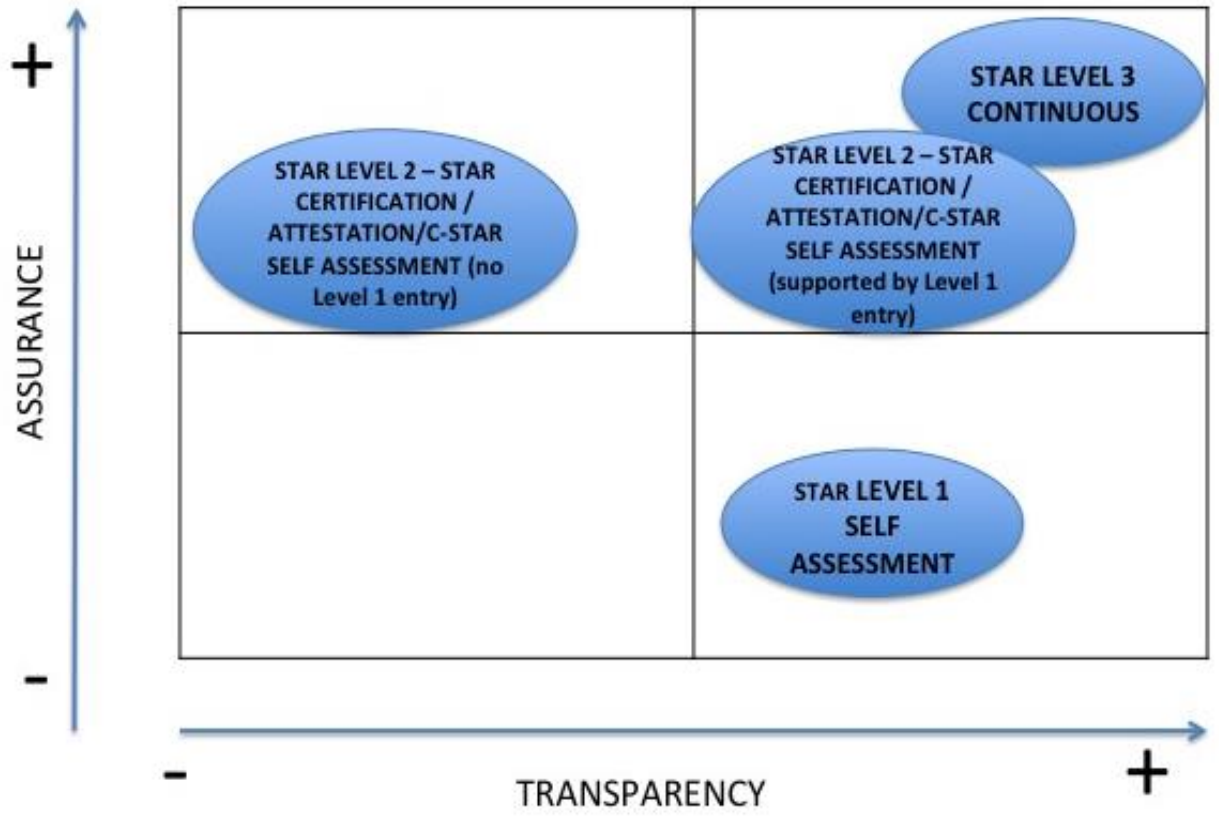


STARプログラム　(2)

STAR　透明性と高い保証

- レベル1
  - プロバイダ自己評価（セルフアセスメント）
- レベル2
  - 第三者認証/監査証明
- レベル3
  - 継続的モニタリング/継続的監査
  - Coming soon

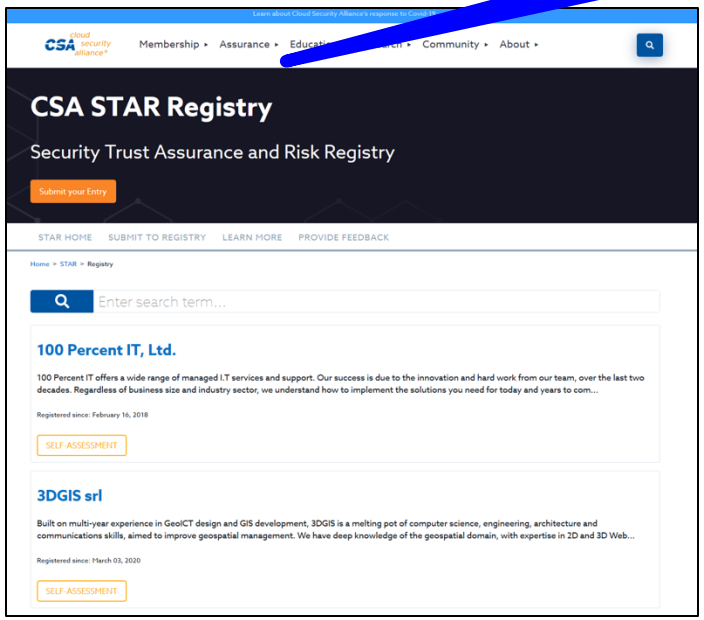
➢ 透明性と高い保証を実現
  ➢ レベル1　＋　レベル2



STARプログラム　(3)　：　STARレベル1

STAR Registry：　プロバイダのセルフアセスメントの結果を公開

公開サイト



プロバイダによるセルフアセスメント

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Microsoft Azure and Dynamics manage Security and Privacy key performance indicators (KPIs) to	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	Shared CSP and CSC	Microsoft Azure's software development practices are aligned with the Microsoft Security Development Lifecycle (SDL)	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	Shared CSP and CSC	Microsoft Azure has established software development and release management processes to control implementation of major changes. Security testing is performed in the	Customers are responsible for developing and following a secure software development program for the customer environment.
AIS-05.2	Is testing automated when applicable and possible?	Yes		Microsoft Azure perform security testing in the implementation, verification and release phases of the	Customers are responsible for developing and following a secure software development program for

引用：　Microsoft AzureのStar1

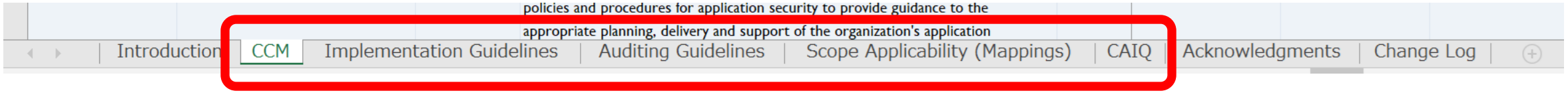
2. Cloud Controls Matrixの全体像

CCMの17ドメイン

A&A	監査と保証
AIS	アプリケーションとインタフェースのセキュリティ
BCR	事業継続管理とオペレーショナルレジリエンス
CCC	変更管理と構成管理
CEK	暗号、暗号化、鍵管理
DCS	データセンターセキュリティ
DSP	データセキュリティとプライバシーのライフサイクル管理
GRC	ガバナンス、リスク、コンプライアンス
HRS	人的リソースセキュリティ
IAM	アイデンティティとアクセス管理
IPY	相互運用性と移植容易性
IVS	インフラストラクチャと仮想化のセキュリティ
LOG	ロギングと監視
SEF	セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジック
STA	サプライチェーン管理、透明性、説明責任
TVM	脅威と脆弱性管理
UEM	ユニバーサル・エンドポイント管理

CCMのEXCELシートの全体像

CCM　EXCELシートのタグ



- CCM Control Specifications and Applicability Matrices
  - 管理策の内容、適用範囲等
- Implementation Guidelines
  - CCMの実装者向けガイド
- Auditing Guidelines
  - CCMの監査者向けのガイド
- Scope Applicability（Mapping）
  - 他の規格とのマッピング
- CAIQ (Consensus Assessment Initiative Questionnaire）
  - CCMの管理策を質問形式にブレークダウンしたもの

CCMの内容　(Control Specifications and Applicability Matrices　：1)

ドメイン

管理策の内容

サービスモデルとの対応
責任共有モデルにおける責任範囲

アーキテクチャの適用レイヤ

CLOUD CONTROLS MATRIX VERSION 4.0.2

Control Domain	Control Title	Control ID	Control Specification	Typical Control Applicability and IaaS	PaaS	SaaS	Architectural Relevance - Cloud Stack Components Phys	Network	Compute	Storage	App	Data
Audit & Assurance - A&A												
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
監査・保証	監査・保証のポリシーと手続き	A&A-01	監査・保証のポリシーと手順と基準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年1回レビューする。	Shared	Shared	Shared	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
監査・保証	独立した評価	A&A-02	少なくとも年1回、関連する基準に従って独立した監査および保証評価を実施する。	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies	Shared	Shared	Shared	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

CCMの内容　(Control Specifications and Applicability Matrices　：２)

対応者/部門

言語選択

cs	Organizational Relevance									
Data	Cybersecurity	Internal Audit	Architecture Team	SW Development	Operations	Legal/Privacy	GRC Team	Supply Chain Management	HR	Language
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	EN
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	JP
TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	EN

注）「言語選択」のフィルターにより、「日本語」「英語」あるいは「両方」の選択が可能

CCMの内容　(Control Specifications and Applicability Matrices)の中味

- Typical Control Applicability and Ownership matrix
  - サービスモデル(IaaS、PaaS、SaaS)の全ての管理策について、標準的な責任共有モデルの所有権と適用可能性を記述
  - CSPとCSCの責任の記述
    - " CSP-Owned "
    - "CSC-Owned "
    - "Shared"：　CSP と CSC の間で責任を共有

- Architectural Relevance and Cloud Stack Components matrix
  - アーキテクチャの適用レイヤ
  - 各管理策のアーキテクチャ上の関連性を記述
    - "物理"、"ネットワーク"、"コンピュート"、"ストレージ"、"アプリケーション"、"データ"。

CCMの内容　(Control Specifications and Applicability Matrices)の中味

- Organizational Relevance matrix
  - 対応者/部門
  - 各管理策と、組織内の各クラウド関連機能によるその実施との関連性を記述
    - サイバーセキュリティ"、"内部監査"、"アーキテクチャチーム"、"SW（ソフトウェア）開発チーム"、"オペレーション"、"法務／プライバシー"、"GRC（ガバナンス／リスク／コントロール）チーム"、"サプライチェーン管理"、"HR（人事）"。

CCMの内容　(Implementation Guidelines、Auditing Guidelines、Scope Applicability（Mapping））

- Implementation Guidelines（実施ガイドライン）
  - CCM管理策の実施方法に関する提案、推奨、例を記述

- Auditing Guidelines（監査者向けガイドライン）
  - CCM 監査を容易にし、指導することを目的
  - 管理策の監査可能性を向上させ、組織がより効率的にコンプライアンスを達成できるようにする。

- Scope Applicability（Mapping）
  - CCM V4と、クラウドコンピューティングクラウドコンピューティングに関連する規格（ISO 27001/2/17/18、NIST SP800-53など）およびベストプラクティス（CIS v8.0）と管理策のマッピング

CCMの内容　(Implementation Guidelines)

実装者向けのガイドライン

実装者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification	Implementation Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Both the cloud service provider (CSP) and cloud service customer (CSC) should develop a "customized integrated framework" of audit and assur This framework should incorporate/demonstrate compliance to leading industry standards and self-imposed business requirements while providi controls to assess the respective cloud environment and corresponding services. At a minimum, audit and assurance policies and procedures should include: a. Audit and assurance functions indicating purposes, responsibilities, authorities, and accountabilities to ensure organizational independence, professional care, audit objectivity, and proficiency, b. Audit and assurance plans, c. Audit development policies and procedures to determine criteria and assertions against which the subject matter will be assessed, quality assurance and supervision, sufficient and appropriate evidence, in accordance with commonly accepted frameworks and audit best practices, d. Audit reporting to communicate audit results and findings, e. Follow-up activities to monitor audit findings implementation progress
監査・保証	監査・保証のポリシーと手続き	**A&A-01**	監査・保証のポリシーと手順と基準について確立、文書化、承認、伝達、適用、評価、維持を少なくとも年1回レビューする。	クラウドサービスプロバイダ（CSP）とクラウドサービスカスタマ（CSC）両者は、監査と保証のポリシーと手順について「カスタマイズされた 発すべきである。 このフレームワークは、各クラウド環境と対応するサービスを評価するために、管理策の適切な範囲を提供しながら、主要な業界標準や自から を、組み込む／証明すべきである。 監査・保証のポリシー及び手続は、最小限、以下を含むべきである。 a. 組織としての独立性、専門的な配慮、監査の客観性、熟練度を確保するための、目的、責任、権限、説明責任などを示した監査や保証機能 b. 監査および保証計画、 c. 監査対象が評価される基準及び主張を決定するための監査展開方針及び手順、品質保証及び監督、一般的に公正妥当と認められたフレーム クティスに従った証拠

... | Introduction | CCM | Implementation Guidelines | Auditing Guidelines | ...

CCMの内容　(Auditing Guidelines)

監査者向けのガイドライン

監査者向け
ガイドライン

CCM CLOUD CONTROLS MATRIX v4.0.10

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update	1. Examine policy and procedures to confirm content adequacy in terms of purpose, authority and accountability, responsibilit communication, reporting, and follow-up. 2. Examine audit charter and determine if independence, impartiality, and objectivity are guaranteed. 3. Examine policy and procedures for evidence of review at least annually.
監査・保証	監査・保証のポリシーと手続き	A&A-01	監査・保証のポリシーと手順と基準について確立、文書化、承認、コミュニケーション、適用、評価、維持を少なくとも年1回レビューする。	1.ポリシーと手順を検証し、目的、権限と責任、責任、計画、コミュニケーション、報告、フォローアップの観点から、内容 する。 2. 監査基本方針を検証し、独立性、公平性、客観性が保証されているかどうかを判断する。 3. 方針と手続を検証し、少なくとも年1回、レビューの証拠を確認する。
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	1. Examine the process to determine standards and regulations applicable to the organization's systems and environments. 2. Determine if the organization maintains and reviews a list of such standards and regulations. 3. Determine if senior management exercises oversight over the independence of the assessment process. 4. Determine if the audit plan is informed by previous assessments, and is scheduled on an annual basis.
監査・保証	独立した評価	A&A-02	少なくとも年1回、関連する基準に従って独立した監査および保証評価を実施する。	1. 組織のシステムと環境に適用される標準と規則を決定するためのプロセスを検証する。 2. 組織がそのような規格や規則のリストを維持し、レビューしているかどうかを判断する。 3. 上級管理職が評価プロセスの独立性を監督しているかどうかを判断する。 4. 監査計画が、前回の評価から情報を得ており、年次ベースで計画されているかどうかを判断する。
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	1. Examine the process for determining the risks applicable to the organization's systems and environments. 2. Determine if a list of such risks is maintained and reviewed. 3. Determine if senior management exercises oversight over the applicable risks. 4. Determine if the audit plan is risk-based, and is scheduled on an annual basis.
監査・保証	リスクベースの計画評価	A&A-03	リスクベースの計画とポリシーに従って、独立した監査と保証評価を実施する。	1. 組織のシステムと環境に適用されるリスクを決定するプロセスを検証する。 2. そのようなリスクのリストが維持され、レビューされているかどうかを判断する。 3. 上級管理職が該当するリスクを監督しているかどうかを判断する。 4. 監査計画がリスクベースであり、年次ベースで計画されているかどうかを判断する。

... Introduction | CCM | Implementation Guidelines | Auditing Guidelines | Scope ...

CCMの内容　(Scope Applicability（Mapping）)

他基準とのマッピング

他基準とのマッピング

CCM CLOUD CONTROLS MATRIX v4.0.5

				CIS v8.0				
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum	Control Mapping	Gap
Audit & Assurance - A&A								
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	8.1	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (8.1) 'Establish and maintain an audit log management process', 'Review and update documentation annually'.	12.1 12.1.1 12.11	Part
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	7.2	Partial Gap	Recommend the full V4 control specification to be used to close the gap. Portion in the mapped control(s) contributing to the partial gap, that is, covering in part the V4 control: (7.2) 'Establish and maintain a risk-based remediation strategy'.	No Mapping	Ful
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and	No Mapping	Full Gap	The full V4 control specification is missing from CISv8.0 and has to be used to close the gap.	No Mapping	Ful

他基準： CIS, PCIDSS, ISO/IEC27001/02/17/18, NIST SP800-53 rev5, etc.

3. CCM関連情報へのリンク

CSAジャパン情報サイト

- CSAジャパン　CCMWGウェブサイト
  - https://www.cloudsecurityalliance.jp/site/?page_id=2048

- CSAジャパン　STAR関連情報ウェブサイト
  - https://www.cloudsecurityalliance.jp/site/?page_id=429

CSAの活動　==　「場」の提供！

様々なワーキンググループ活動の「場」

自由な情報発信の「場」

https://cloudsecurityalliance.jp

ご意見、ご質問等は、以下にご連絡ください。

mmorozumi@cloudsecurityalliance.jp

（本メールアドレスには、S/MIME電子証明書を付与してお送りしますので、安心して情報交換できます）

ありがとうございました！