Agenda

A. **Introduction to Speakers**
B. **What is CSA STAR?**
C. **CSA STAR Levels of Assessment**
D. **CSA STAR Domains**
E. **STAR Registry**
F. **The Italian Mandate**
G. **Q&A**

A. Introduction to our Speakers

Speakers

Daniele Catteddu,

Chief Technology Officer, Cloud Security Alliance

Daniele is an information security and risk management practitioner, a technologies expert, and a privacy evangelist with 15+ years of experience. He is the co-founder and executive of the CSA Open Certification Framework / STAR Program.

Ashish Kirtikar,

ControlCase President, UK & Europe

Ashish has 15+ years of experience and proficiency in information & network security, information risk management, cyber security, resilience, security architecture design, information security auditing, and governance within stipulated deadlines.

B. WHAT IS CSA STAR?

What is CSA STAR?

Founded in 2011, the **CSA STAR** stands for Security, Transparency, Assurance and Risk program.

STAR encompasses the key principles of **transparency**, **rigorous auditing**, and **harmonization of standards** outlined in the **Cloud Controls Matrix (CCM).**

Additionally, publishing to the CSA STAR Registry allows organizations to show current and potential customers their security and compliance posture, including the regulations, standards, and frameworks they adhere to.
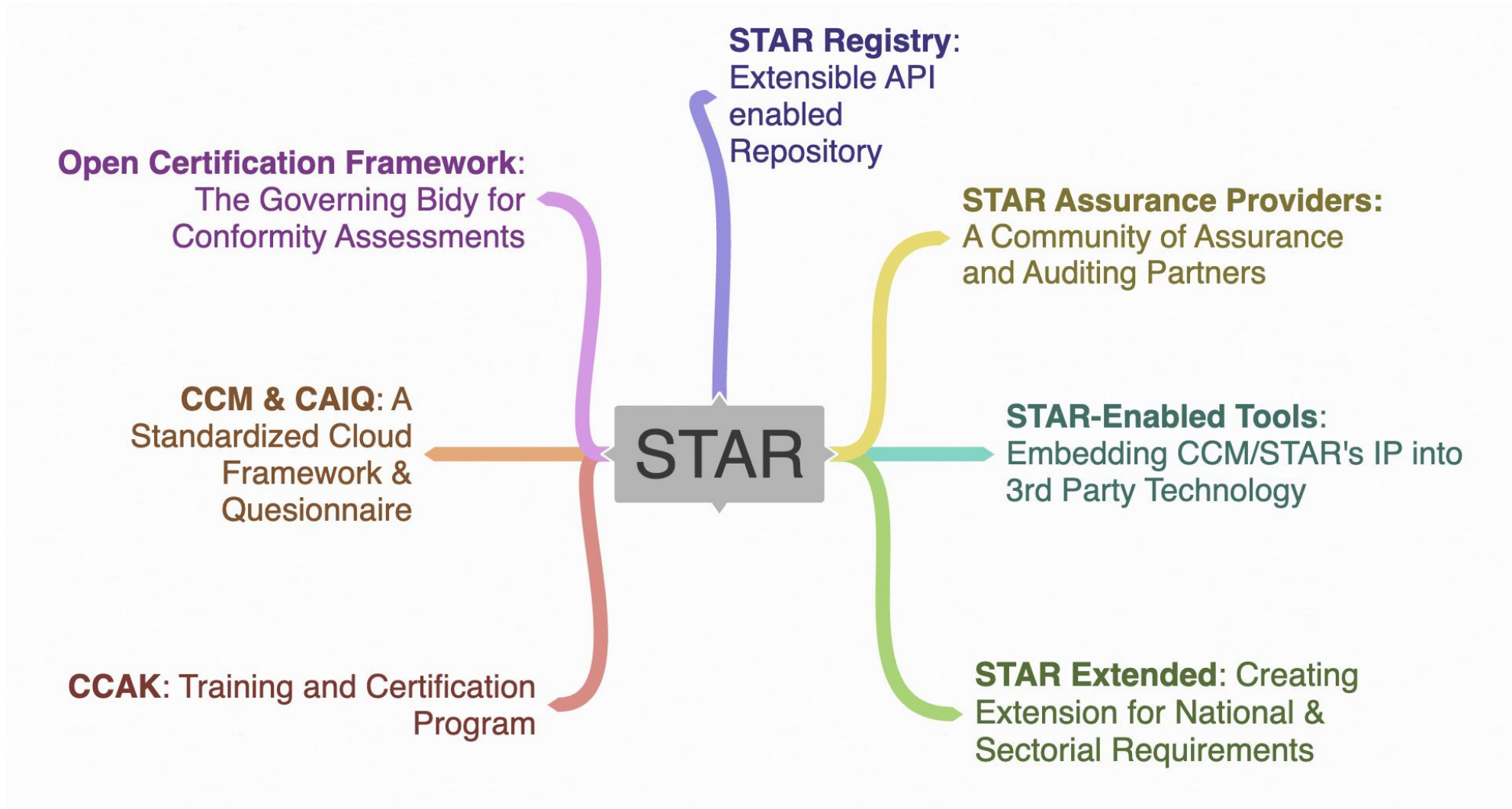
Why the STAR Program

The cloud computing market is very heterogenous with common needs and issues:

- **How to define trust in the cloud?**

- **How to foster accountability?**

- **How to evaluate risk?**

- **How to measure assurance?**

- **How to simplify compliance and procurement?**

- The goal of the STAR Program is to support any organization to effectively and efficiently address those question

STAR Pillars and Ecosystems

STAR Registry: Extensible API enabled Repository

Open Certification Framework: The Governing Bidy for Conformity Assessments

STAR Assurance Providers: A Community of Assurance and Auditing Partners

CCM & CAIQ: A Standardized Cloud Framework & Quesionnaire

STAR

STAR-Enabled Tools: Embedding CCM/STAR's IP into 3rd Party Technology

CCAK: Training and Certification Program

STAR Extended: Creating Extension for National & Sectorial Requirements

C. CSA STAR LEVELS OF ASSESSMENT

CSA STAR Levels of Assessment

CSA STAR Level 1: Self-Assessment

Organizations can submit one or both the security and privacy self-assessments.

Organizations should pursue Level 1 if they are:
- Operating in a low-risk environment.
- Wanting to offer increased transparency around the security controls they have in place.
- Looking for a cost-effective way to improve trust and transparency.

CSA STAR Level 2: Third Party Audit

Allows organizations to build off other industry certifications and standards to make them specific for the cloud.

Organizations should pursue Level 2 if they are:
- Operating in a medium-to-high risk environment
- Already holding or adhering to the following: **ISO27001**, **SOC 2**
- Looking for a cost-effective way to increase assurance for cloud security and privacy.

STAR Certification Framework

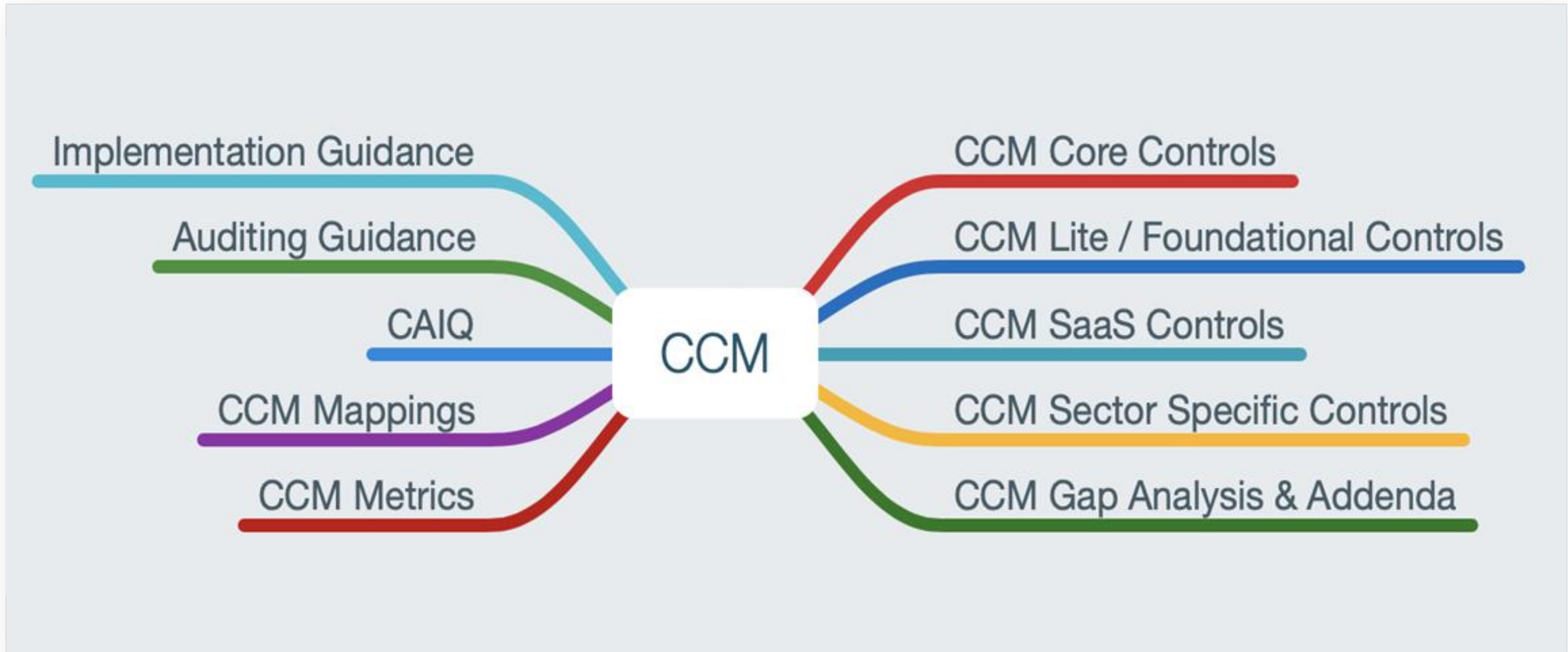| TYPE OF AUDIT		AUDIT FREQUENCY	Security	Privacy
	STAR Level 3	● ● ●	Continuous Auditing	
	STAR Level 2 Continuous	● ● ○	Level 2 + Continuous Self-Assessment	
	STAR Level 2		3rd Party Certification	GDPR CoC Certification
	STAR Level 1 Continuous	● ○ ○	Continuous Self-Assessment	
	STAR Level 1		Self-Assessment	GDPR CoC Self-Assessment

TRANSPARENCY & ASSURANCE

D. CSA STAR DOMAINS

What are the CSA Star Domains?

A&A	Audit & Assurance	**IAM**	Identity & Access Management
AIS	Application & Interface Security	**IPY**	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	**IVS**	Infrastructure & Virtualization
CCC	Change Control & Configuration Management	**LOG**	Logging and Monitoring
CEK	Cryptography, Encryption and Key Management	**SEF**	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	**STA**	Supply Chain Mgmt, Transparency & Accountability
DSP	Data Security and Privacy	**TVM**	Threat & Vulnerability Management
GRM	Governance, Risk Management and Compliance	**UEP**	Universal EndPoint Management
HRS	Human Resources Security		

What are the CSA Star Domains?

Implementation Guidance

Auditing Guidance

CAIQ

CCM Mappings

CCM Metrics

CCM

CCM Core Controls

CCM Lite / Foundational Controls

CCM SaaS Controls

CCM Sector Specific Controls

CCM Gap Analysis & Addenda

E. THE STAR REGISTRY

STAR Registry

SECURITY TRUST ASSURANCE RISK REGISTRY

LAUNCHED IN 2011
CSA STAR is the first step in **improving transparency and assurance** in the cloud

TRUSTED & AUTHORITATIVE
Has the ambition to be the trusted and authoritative repository of Cloud-GCR related data

PUBLICLY ACCESSIBLE & SEARCHABLE
The Registry allows cloud customers to review the security and privacy controls provided by cloud computing offerings

KNOW CLOUD SERVICE PROVIDER'S POSTURE
Helps **users** to **assess** the **security** AND **PRIVACY** **posture** of providers BASED ON CSA STANDARDS AND BEST PRACTICES
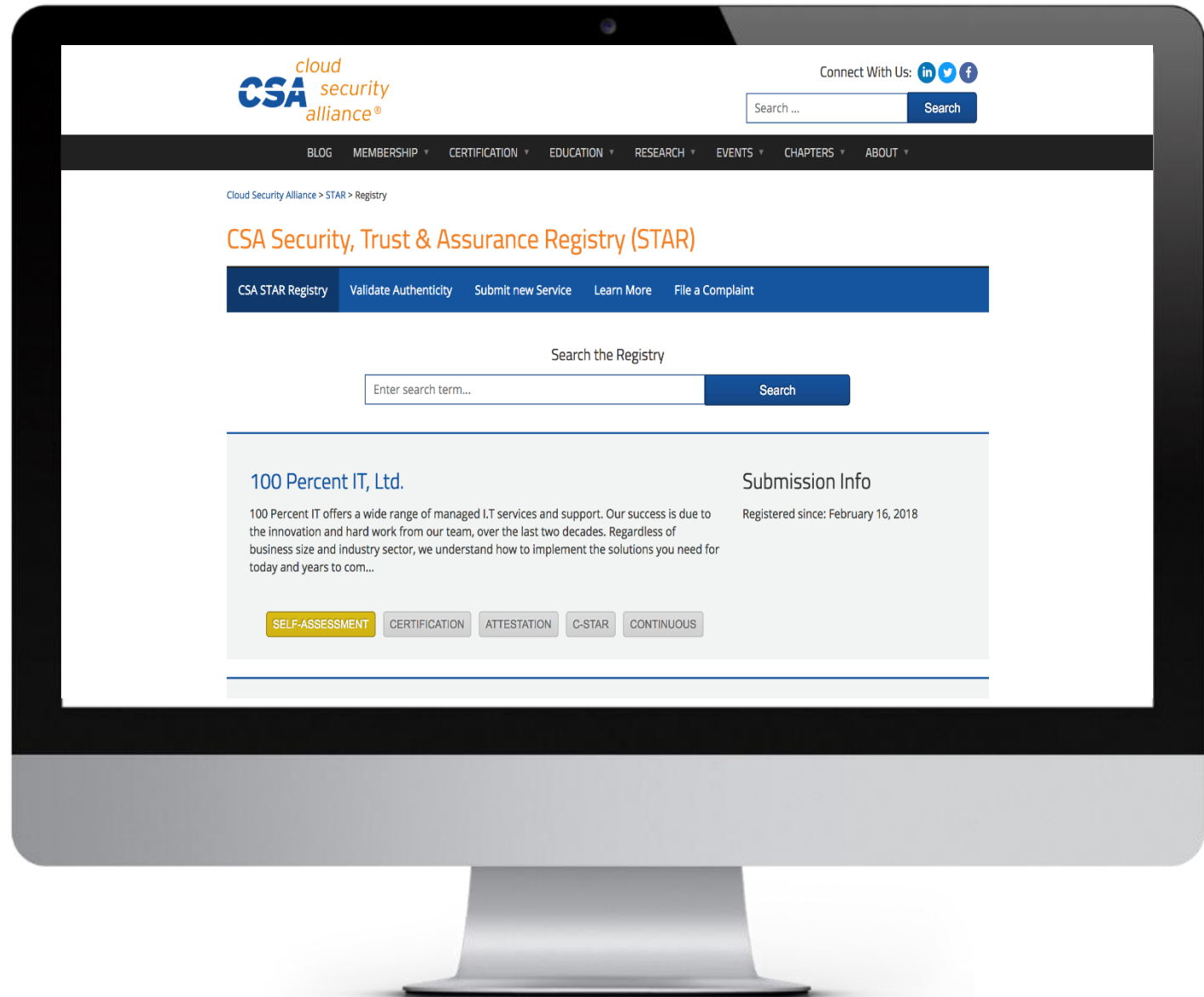
FILE MANAGEMENT
Suitable for all categories business and personal presentation

CSA cloud security alliance ®

CSA STAR
Security, Trust & Assurance
Registry

STAR Registry

SECURITY TRUST ASSURANCE
RISK REGISTRY

F. THE ITALIAN MANDATE

The Italian Mandate

Italy has taken a step forward in recognizing the importance of cloud security by making it clear that they're **adopting the Cloud Controls Matrix and STAR Program as key pillars** within their framework for defining security requirements for cloud services offered for public administration.

The Italian Mandate Overview

The Italian Agency for National Cybersecurity (ACN) recently reaffirmed the **key role of the CCM and the STAR Program** as part of the definition of security requirements for cloud services offered for public administration and their certification.

In 2022, the Italian Government published a tender for the creation of a National Cloud via Public-Private Partnership, **mandating compliance with CSA STAR Level 2.**

The Italian Mandate Overview

The new minimum-security requirements, communicated by the ACN, apply to data classified into **3 levels of importance**:

Ordinary

Critical

Strategic

G. Q & A

THANK YOU FOR THE OPPORTUNITY TO CONTRIBUTE TO YOUR IT COMPLIANCE PROGRAM.

www.controlcase.com

contact@controlcase.com