Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Computer Engineering
(full name of faculty)
Computer Systems and Network Department
(full name of department)

QUALIFYING PAPER

For the degree of

Masters in Computer Engineering
(degree name)

topic: **"Methods for increasing the security level of the information and Communication system of visa service"**

Submitted by: sixth year student 6 , group ICIm-62

specialty *123"Computer Engineering"*

6.050102 "Computer Engineering"
(code and name of specialty)

	(signature)	Aboah A. H (surname and initials)
Supervisor	(signature)	Lutskiv A. M (surname and initials)
Standards verified by	(signature)	(surname and initials)
Head of Department	(signature)	(surname and initials)
Reviewer	(signature)	(surname and initials)

Ternopil 2021

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Computer Engineering
(full name of faculty)

Department Computer Systems and Networks Department
(full name of department)

APPROVED BY
Head of Department

(signature) (surname and initials)
« » 20_21__

ASSIGNMENT
for QUALIFYING PAPER

for the degree of Masters in Computer Engineering
(degree name)

specialty *6.050102 "Computer Engineering"*
(code and name of the specialty)

student Aboah Angel Henrietta
(surname, name, patronymic)

1. Paper topic **"Methods for increasing the security level of the information and Communication system of visa service"**

Paper supervisor
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of «____» ____________ 20_21__ № ____________

2. Student's paper submission deadline 23/12/21

3. Initial data for the paper "Methods for increasing the security level of the information and Communication system of visa service"

4. Paper contents (list of issues to be developed)
Securing Visa Service
Design security of visa service taking into account GDPR Regulations
Audit security in visa service
Implementation guidelines of Metrics at visa service
Conclusions and recommendations of securing organizations

5. List of graphic material (with exact number of required drawings, slides)
Figure 1.2 - Framework Management Structure of Visa Service
Figure 1.8 - Cloud Control Matrix Specification, Interface security, Audit and Assurance
Figure 2.2 - Data security Journey system
Figure 2.5 - Cloud Control Matrix Mapping
Figure 2.9 - CAIQ Answer
Figure 3.1 - Main branch of visa processing system
Figure 3.4 - Automated Check-in security
Figure 3.5 - Smart Airport and visa System
Figure 3.9 - SerpentCS Tracking
Figure 3.17 - Metric AIS-07

6. Advisors of paper chapters

hapter	Advisor’s surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
1	Andriy A. M. Professor		
2	Andriy A. M. Professor		
3	Andriy A. M. Professor		
4	Lazaryuk V. Associate Professor		

7. Date of receiving the assignment ____

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	Research materials (topic, books, links etc.)	10/10/21-10/25/21	Completed
2	Abstract, Introduction and Chapter 1 “infrastructural Model of visa service”	10/26/21-10/30/21	Completed
3	Chapter 2 Audit and physical Security at Visa service	11/01/21-11/20/21	Completed
4	Chapter 3 Special Part Implementation Guidelines	11/21/21-11/31/21	Completed
5	Chapter 4 Labor Safety	12/01/21-12/16/21	Completed
6	Conclusion and References	12/17/21-12/22/21	Completed

Student ____________ (signature) Aboah A. H (surname and initials)

Paper supervisor ____________ (signature) Lutskiv A.M (surname and initials)

ABSTRACT

Methods for increasing the security level of the information and Communication system of Visa Service//Master Thesis// Angel Henrietta Aboah // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Computer Systems and Networks Department, group ICIm-62 // Ternopil, 2021 // p.–60, fig.-43, tab.–0, draw. –0, append. –3, ref.–12.

Key words: INFORMATION, SECURITY, METHODS, VISA FACILITATION SERVICE CENTER, INFRASTRUCTURE, SMART TRAVEL, COMMUNICATION SYSTEM, VISA TROUBLES & SOLUTIONS, CLOUD CONTROL MATRIX, AUDIT

Designated object – Methods for increasing the security level of the information and Communication system of Visa Service.

The research is based on Methods for increasing the security level of the information and Communication system of Visa Service. This research is to help improve the work at Visa Service center and how to improve the security of the information and communication system at Visa Service Center. The key problems of information security of travel agencies and visa service centers due to information threats are identified. The essence and ways of providing certain components of information security of tourism are characterized. The prospects of further research of information and communication aspects of tourism security are determined. Routers, switches, firewalls, warehouses, servers, and implementation controllers are the key components of a communications infrastructure system.

TABLE OF CONTENT

INTRODUCTION

Significance of the findings. In spite of the good and reliable services that travel companies have provided to people across the world, there has been a growing concern about the client's information and how secure the documents received at Visa Service centers are. There is a growing furor about the poor process of visa applications, which seem to have reached an all-time low. The application systems for obtaining a visa, extension, settlement or citizenship are mostly online and outsourced. Nevertheless, far from becoming more efficient, there is growing evidence that the visa system is not fit for purpose, as the security of client's information has been the major concern of many recently. Visa services reduce most of the paperwork required to apply for a visa to visit a particular country. If you do not know how to get a visa for an upcoming trip or you just want to make sure everything is filed correctly, visa service companies can do the job for you. Visa service centers will make sure all required paperwork is filled, signed, and delivered to the right place. Passport photos are checked for faults, and their staff is there to answer any questions that you may have. These companies also often do things like renewing your passport and handling any international mail required for your visa.

The security of information at Visa Service center is connected to a number of measures taken to prevent the transfer and destruction of those who are not authorized. The visa service settings have been the most fundamental requirement of individuals and institutions. High-level measures should be taken against cyber-attacks detected. Selecting as well as measuring important security attributes of an information system presents a significant challenge. While traditional security auditing processes can rely on a large body of knowledge and well-established references such as ISO/IEC 27001, ISO/IEC 27017 or the CSA CCM, there is no such foundation available for continuous auditing of cloud services. Proposed metrics were designed to be consistent with the newly released CSA Cloud Control Matrix v4 controls (CCMv4). These metrics aim to support internal CSP governance, risk, and compliance activities and provide a useful baseline for service-level agreement transparency.

The goals and tasks of the study. This is to develop methods for increasing the security level of the information and communication system of visa service.

Achieving this goal requires the following tasks:

- Securing visa service
- Analysis of data flows in Visa service
- Design security of visa service
- Audit/Cloud Security in visa service
- Implementation's guidelines of metrics at visa service

The objective section of the study is the processing of development and improvement of visa service information security.

The subjective section of the study is the security standards and regulations, software tools for security audit, security guides.

Technical aspect of the acquired results:

- Choosing proper security metrics to measure security level of visa service.
- The applicable importance of the solutions obtained.

Suggested metrics and conclusions allowed to develop secure visa service computer network infrastructure.

Testing of the thesis.

The results of the master's thesis work were tested at international conferences:

- VIII International Scientific and Technical Conference of Students "Resolving Machine Learning in Distributed Memory Environment".
- VII "Development of secured Cloud Data processing environments".

Description of work. The work comprises of a detailed discussion of the theme and diagrams (Figures) inclusive. The thesis is composed of an introduction, three sections, conclusions, references and appendices. Scope of work: detailed discussion-sheet. A4 measurement of paper, diagrams (Figures) part – 5 sheets A1.

CHAPTER 1
ANALYSIS OF THE SUBJECT AREA OF SECURITY AT VISA SERVICES

1.1 Review of Visa Facilitation Service

Visa Facilitation Service is the biggest application service specialized for governments over the world. Visa Facilitation Service is the trusted partner of different diplomatic organization serving 144 countries through more than 3,400 application centers in five continents.

1.1.2 Taking into account GDPR regulations

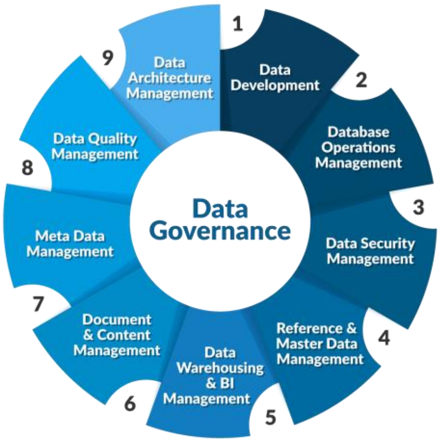

Data Governance
1
Data Development
2
Database Operations Management
3
Data Security Management
4
Reference & Master Data Management
5
Data Warehousing & BI Management
6
Document & Content Management
7
Meta Data Management
8
Data Quality Management
9
Data Architecture Management

Figure 1.1 – GDPR Regulations

Occupying the service areas of consular, data accumulation is a certain part of the center’s business plans. The guarantee of the data of customers are carefully handled in a secure manner in with international privacy regulations such as General Data Protection Regulation. The center is obligated to making sure the standards of information security and privacy are sustained.

1.2 Business Model

Visa Facilitation Service is a provider of visas, passports, and other diplomatic services and help governments to manage tasks including data processing and visa application processing. At the Visa Facilitation Service, its goal is to improve the customer experience by making the visa application process seamless as possible. It deals with people business and has built a strong customer-focused culture.

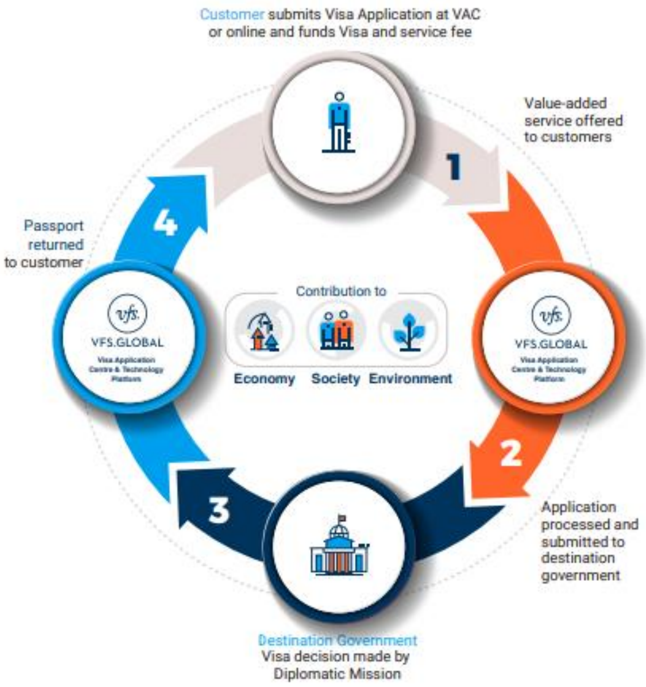
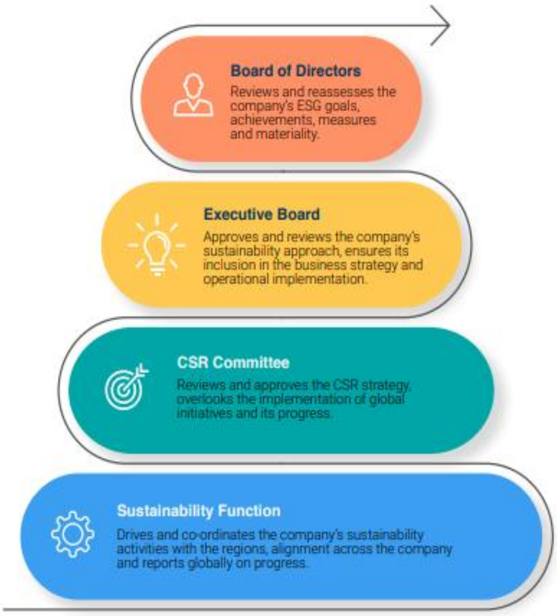

Customer submits Visa Application at VAC or online and funds Visa and service fee
1
Value-added service offered to customers
VFS.GLOBAL
Visa Application Centre & Technology Platform
2
Application processed and submitted to destination government
3
Destination Government
Visa decision made by Diplomatic Mission
VFS.GLOBAL
Visa Application Centre & Technology Platform
4
Passport returned to customer
Contribution to
Economy
Society
Environment

Figure 1.2 - Driving process efficiency across operations

The Visa service is important for the privacy and security of the Visa Facilitation service. For this reason, Visa facilitation service does not store any customer data beyond the visa application process. In line with its core values Integrity, Commitment, and Entrepreneurship, it uses strict protocols around the entire application process as well as the enrolment and encryption of biometric information. However, the changing needs of today’s consumer main focus is to become future ready process, which may include document pre-checks or payments.



Board of Directors

Reviews and reassesses the company's ESG goals, achievements, measures and materiality.

Executive Board

Approves and reviews the company's sustainability approach, ensures its inclusion in the business strategy and operational implementation.

CSR Committee

Reviews and approves the CSR strategy, overlooks the implementation of global initiatives and its progress.

Sustainability Function

Drives and co-ordinates the company's sustainability activities with the regions, alignment across the company and reports globally on progress.

Figure 1.3 - Framework Management structure of Visa service

Visa Facilitation Service adheres to the 10 principles of the UN Global Compact. The key objectives for sustainability include:

- forming continuous robust sustainability processes;
- Tracking and reporting the functional indicators including ethics, corruption etc.
- forming awareness for employees
- developing sustainability strategy.

Figure 1.4 - Sustainability Governance Structure

The functional indicator targets are reviewed annually by Board of Directors.

1.3 Materiality

This existing materiality assessment was reviewed and updated in 2020. The stakeholders are invited to participate in the assessment that is carried out through anonymous survey. With these statistics, it was rated 18 topics according to their significance and impact on business at visa service.

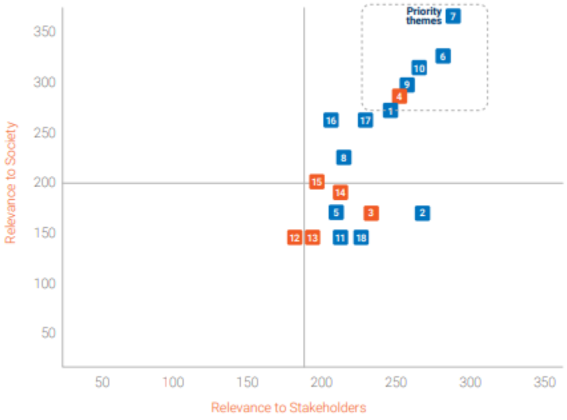
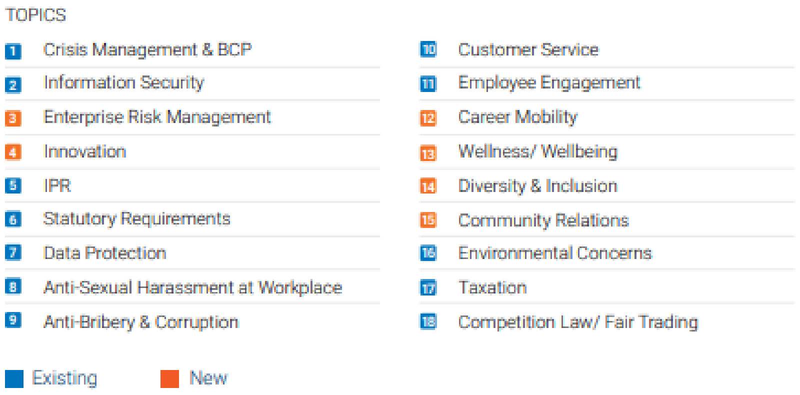


Figure 1.5 - Materiality graph of Stakeholders

The main topics that were ranked are listed below:

- Data Protection
- Statutory Requirements
- Information Security
- Customer Service
- Innovation
- Crisis Management & Business Continuity Plan (BCP)



TOPICS

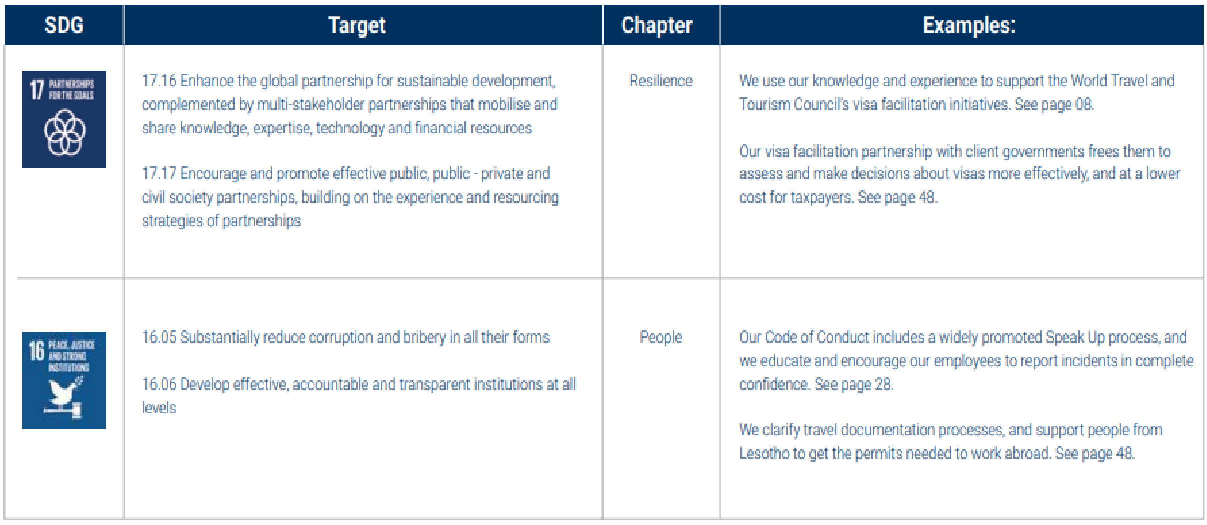
1	Crisis Management & BCP	10	Customer Service
2	Information Security	11	Employee Engagement
3	Enterprise Risk Management	12	Career Mobility
4	Innovation	13	Wellness/ Wellbeing
5	IPR	14	Diversity & Inclusion
6	Statutory Requirements	15	Community Relations
7	Data Protection	16	Environmental Concerns
8	Anti-Sexual Harassment at Workplace	17	Taxation
9	Anti-Bribery & Corruption	18	Competition Law/ Fair Trading

🟦 Existing 🟥 New

Figure 1.6 - Materiality Matrix

1.4 Sustainable Development Goals

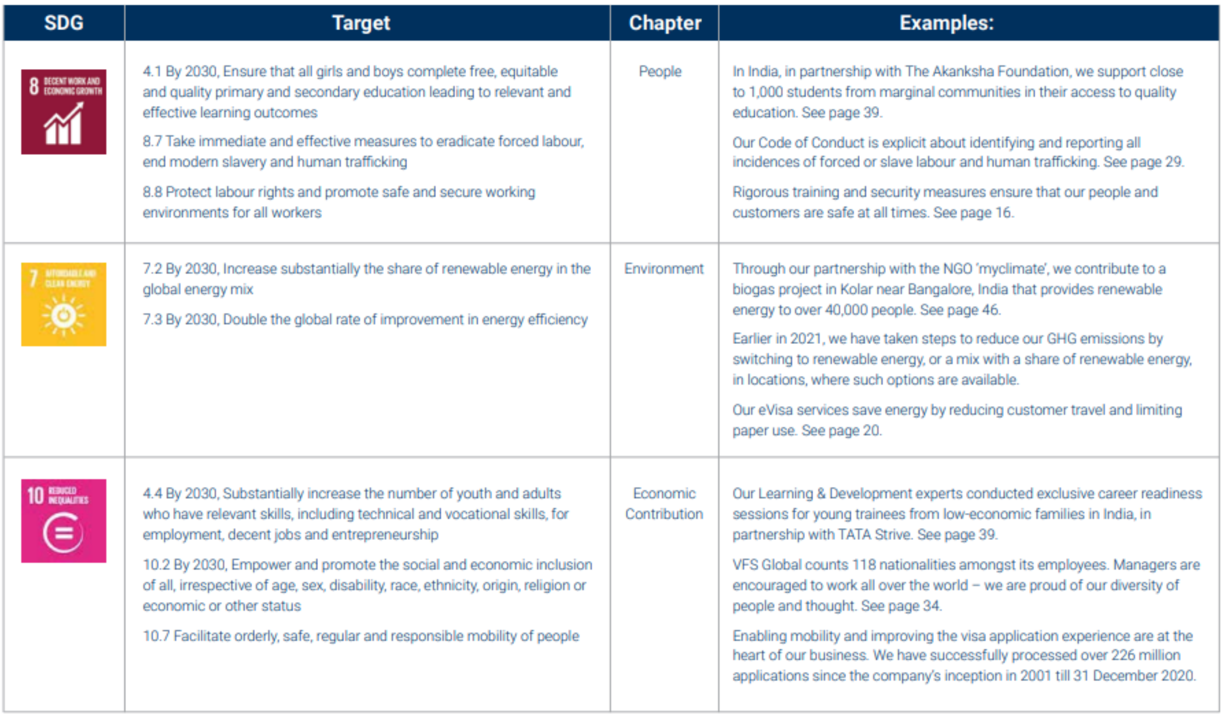
Visa Facilitation Service is keen to conducting business that benefits the communities in which it operates. In the table below is a mapped business activities based on stakeholder and society’s relevance. This allows the center to be aligned with its international sustainability priorities.



SDG	Target	Chapter	Examples:
17 PARTNERSHIPS FOR THE GOALS	17.16 Enhance the global partnership for sustainable development, complemented by multi-stakeholder partnerships that mobilise and share knowledge, expertise, technology and financial resources 17.17 Encourage and promote effective public, public - private and civil society partnerships, building on the experience and resourcing strategies of partnerships	Resilience	We use our knowledge and experience to support the World Travel and Tourism Council's visa facilitation initiatives. See page 08. Our visa facilitation partnership with client governments frees them to assess and make decisions about visas more effectively, and at a lower cost for taxpayers. See page 48.
16 PEACE, JUSTICE AND STRONG INSTITUTIONS	16.05 Substantially reduce corruption and bribery in all their forms 16.06 Develop effective, accountable and transparent institutions at all levels	People	Our Code of Conduct includes a widely promoted Speak Up process, and we educate and encourage our employees to report incidents in complete confidence. See page 28. We clarify travel documentation processes, and support people from Lesotho to get the permits needed to work abroad. See page 48.

Figure 1.7 - Sustainable Development Goals

The table below sums up the targets identified where visa service is making its impact. Its contribution to the goals is described in the relevant section of the table, with examples.



SDG	Target	Chapter	Examples:
8 DECENT WORK AND ECONOMIC GROWTH	4.1 By 2030, Ensure that all girls and boys complete free, equitable and quality primary and secondary education leading to relevant and effective learning outcomes 8.7 Take immediate and effective measures to eradicate forced labour, end modern slavery and human trafficking 8.8 Protect labour rights and promote safe and secure working environments for all workers	People	In India, in partnership with The Akanksha Foundation, we support close to 1,000 students from marginal communities in their access to quality education. See page 39. Our Code of Conduct is explicit about identifying and reporting all incidences of forced or slave labour and human trafficking. See page 29. Rigorous training and security measures ensure that our people and customers are safe at all times. See page 16.
7 AFFORDABLE AND CLEAN ENERGY	7.2 By 2030, Increase substantially the share of renewable energy in the global energy mix 7.3 By 2030, Double the global rate of improvement in energy efficiency	Environment	Through our partnership with the NGO 'myclimate', we contribute to a biogas project in Kolar near Bangalore, India that provides renewable energy to over 40,000 people. See page 46. Earlier in 2021, we have taken steps to reduce our GHG emissions by switching to renewable energy, or a mix with a share of renewable energy, in locations, where such options are available. Our eVisa services save energy by reducing customer travel and limiting paper use. See page 20.
10 REDUCED INEQUALITIES	4.4 By 2030, Substantially increase the number of youth and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship 10.2 By 2030, Empower and promote the social and economic inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status 10.7 Facilitate orderly, safe, regular and responsible mobility of people	Economic Contribution	Our Learning & Development experts conducted exclusive career readiness sessions for young trainees from low-economic families in India, in partnership with TATA Strive. See page 39. VFS Global counts 118 nationalities amongst its employees. Managers are encouraged to work all over the world – we are proud of our diversity of people and thought. See page 34. Enabling mobility and improving the visa application experience are at the heart of our business. We have successfully processed over 226 million applications since the company's inception in 2001 till 31 December 2020.

Figure 1.8 - Sustainable Development Goals

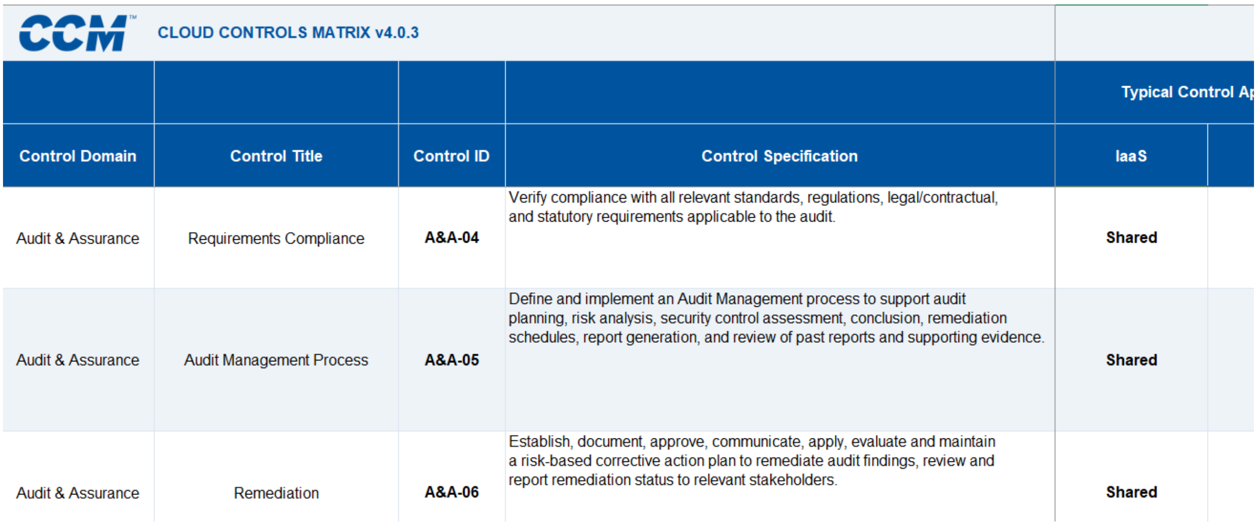
Sustainability at the Visa Facilitation Service means working ethically. Visa Facilitation Service is agile and resilient to the changing market needs, the one aspect that that defines the way visa facilitation service conducts business Sustainability.

1.5 Design Security of Visa Service

Visa organizations that use metrics can give relevant stakeholders a view into their security and privacy practices. Increased transparency fosters trust and accountability within the overall supply chain as each member of the chain can build more reliable service level agreements. The benefits include the relationship between the CSP, its customer and regulatory authorities. Increased level of transparency allows cloud customers to improve their due diligence approach and accountability programs, which will be based on clearer data. The ability to measure control performance at required time intervals is supported by metrics. Both internal and external stakeholders benefit from continuous auditing:

- Internally, visa organizations can use metrics and objectives to measure the performance of their information security. Continuous improvement can be achieved by maintaining a proper security baseline.

- Externally, the visa organizations can use metrics to monitor security and share results with their external stakeholders and their customers who seek assurance that the organization’s information security continuously meets expected levels. The process can be made very efficient by automation and application programming interfaces.



CCM CLOUD CONTROLS MATRIX v4.0.3

				Typical Control Ap
Control Domain	Control Title	Control ID	Control Specification	IaaS
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Shared
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.	Shared
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 report remediation status to relevant stakeholders.	Shared

Figure 1.9 - Cloud control matrix specification

The metrics presented in the metric catalog are linked to CCMv4, which was released in January 2021. The Cloud Controls Matrix is CSA’s flagship cybersecurity framework for cloud computing, featuring 197 control objectives categorized in 17 security domains.

i. Security domains

Each control is described by a:

a. Control Domain: the name of the domain to which the control pertains.

b. Control Title: the title of the control.

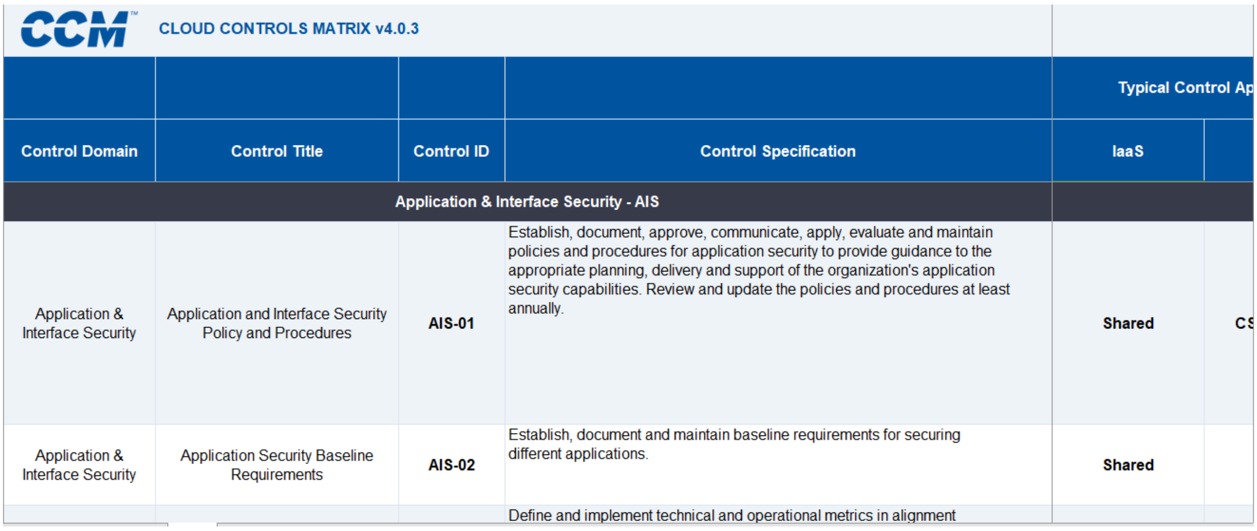
c. Control ID: the control identifier.

d. Control Specification: the requirement(s) description of the control.

e. In addition, this tab includes the following sections (groups of columns)

This group of columns describes the typical applicability of controls for the three main cloud delivery models: IaaS, PaaS and SaaS. The section discusses the typical SSRM-based (Shared Security Responsibility Model) allocation of responsibilities for the implementation of a given CCM control between a cloud service provider and a cloud service customer. The matrix clarifies whether a control’s responsibility should be

CSP-Owned, CSC-Owned or Shared. It is important that both the control applicability to IaaS, PaaS and SaaS models and the control ownership attributions be meant to represent a high-level simplification.

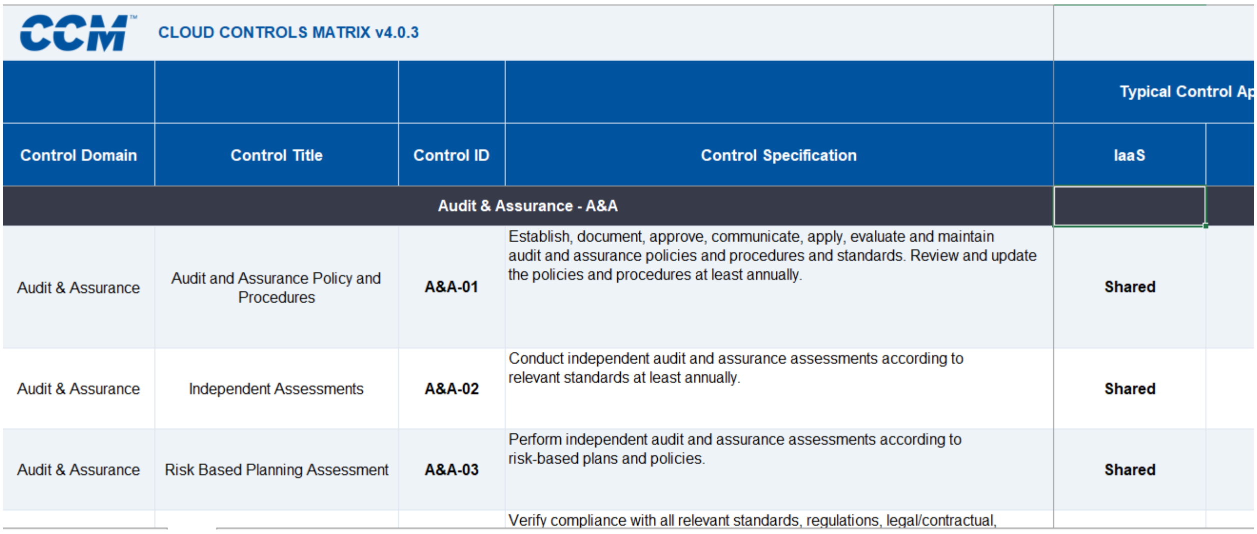


CLOUD CONTROLS MATRIX v4.0.3

				Typical Control Ap	
Control Domain	Control Title	Control ID	Control Specification	IaaS	
Application & Interface Security - AIS					
Application & Interface Security	Application and Interface Security Policy and Procedures	AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Shared	CS
Application & Interface Security	Application Security Baseline Requirements	AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Shared	
			Define and implement technical and operational metrics in alignment		

Figure 1.10 - CCM Interface Security

The CCM user should revise these attributions depending on the contractually agreed SSRM for the particular cloud environment. This group of columns indicates the architectural relevance of each CCM control per cloud stack component from the perspective of the CSA Cloud Reference Model. This section focuses on components, including physical, network, compute, storage, application, and data. The “relevance box” associated with each component is marked as “TRUE” if the control is relevant to a component, and “FALSE” if it isn’t. The architectural relevance is meant to represent a high-level simplification. The CCM user should revise those attributions depending on the cloud environment and technologies used.



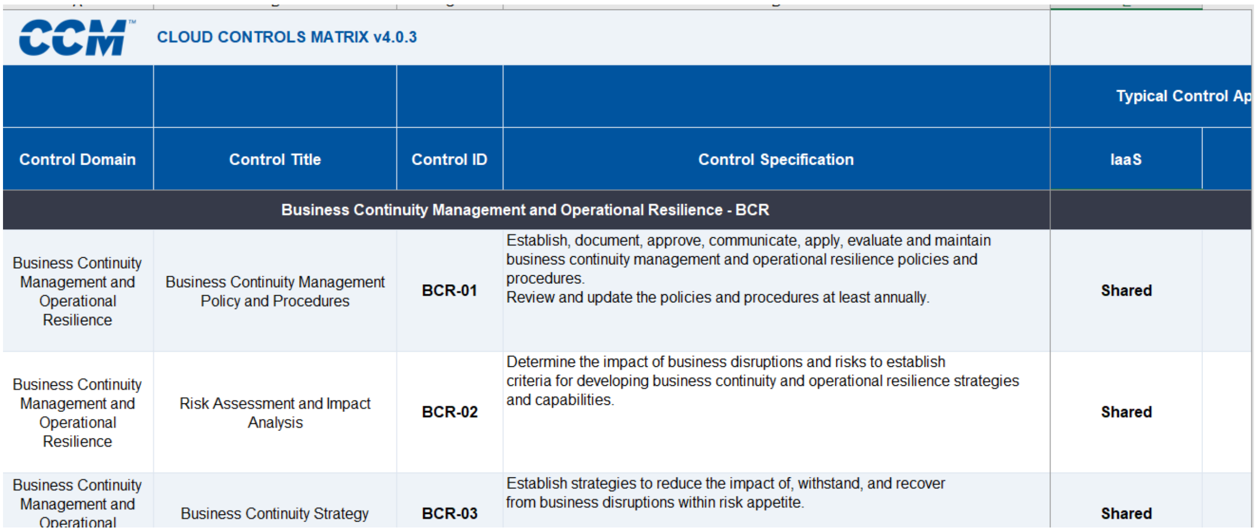
CCM CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Typical Control Ap IaaS
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
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Shared
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Shared
			Verify compliance with all relevant standards, regulations, legal/contractual,	

Figure 1.11 - Audit and Assurance

b. Organization relevance

This group of columns indicates the relevance between the CCM control and its implementation by the cloud relevant functions within an organization. The functions included are Cybersecurity, Internal Audit, Architecture Team, Software Dev Team, Operations, Legal/Privacy, Governance/Risk/Control, Supply Chain Management, and Human. The “relevance box” associated with each component is marked as “TRUE” if the control is relevant to a component and “FALSE” if it isn’t. The organizational relevance is meant to represent a high-level simplification. The user of the CCM should revise these attributions depending on the particular cloud environment and organizational structure.

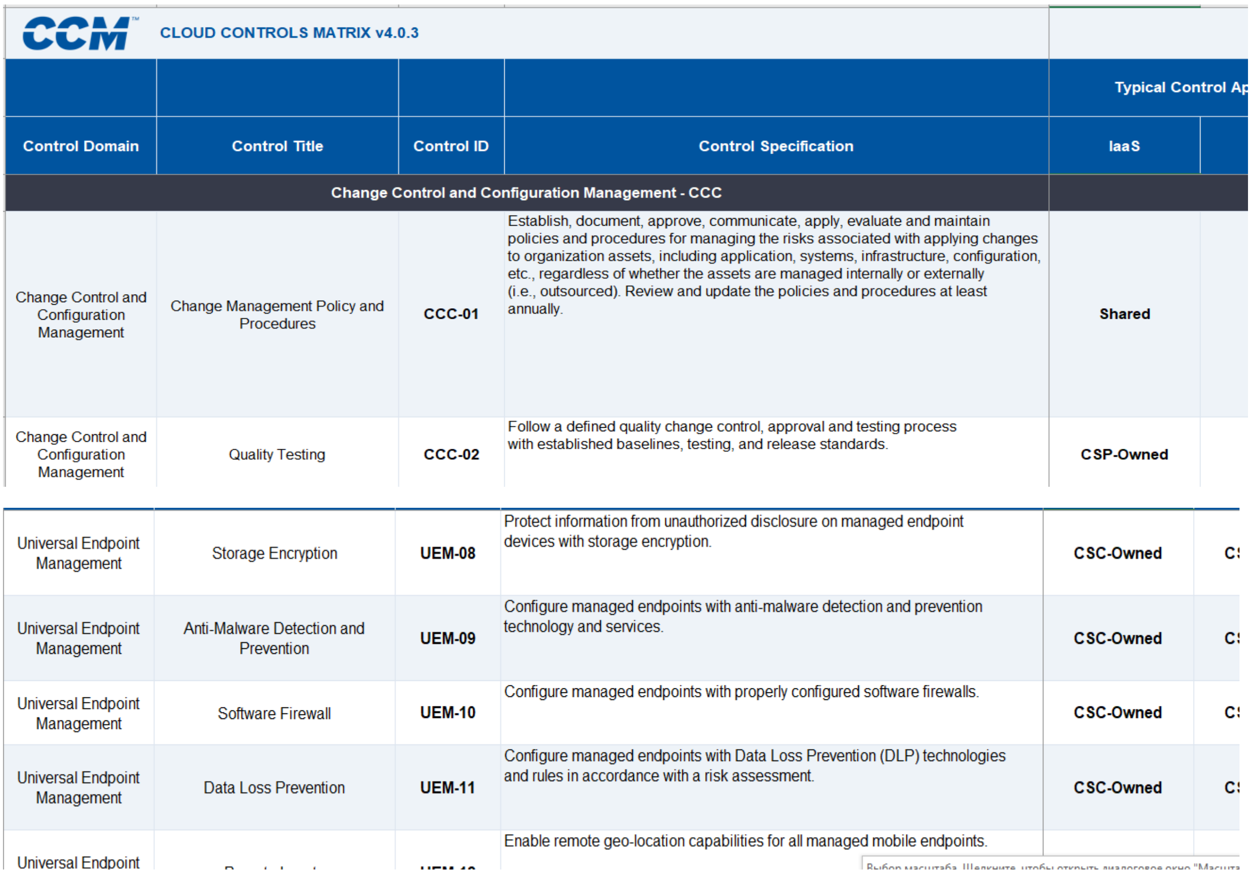


CCM CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Typical Control Ap IaaS
Business Continuity Management and Operational Resilience - BCR				
Business Continuity Management and Operational Resilience	Business Continuity Management Policy and Procedures	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Shared
Business Continuity Management and Operational Resilience	Risk Assessment and Impact Analysis	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Shared
Business Continuity Management and Operational	Business Continuity Strategy	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Shared

Figure 1.12 - Business Continuity Matrix

The metrics catalog we publish in this first release contains metrics related to a subset of the CCM control. The metrics catalog is meant to be a “living document” and additional metrics and extended coverage of the CCM controls will be added over time. The metrics provided in the CSA catalog are not the only way to measure a CCM implementation effectiveness, but rather a possible way to achieve such a goal. Some organizations might use different metrics to achieve the same goals.



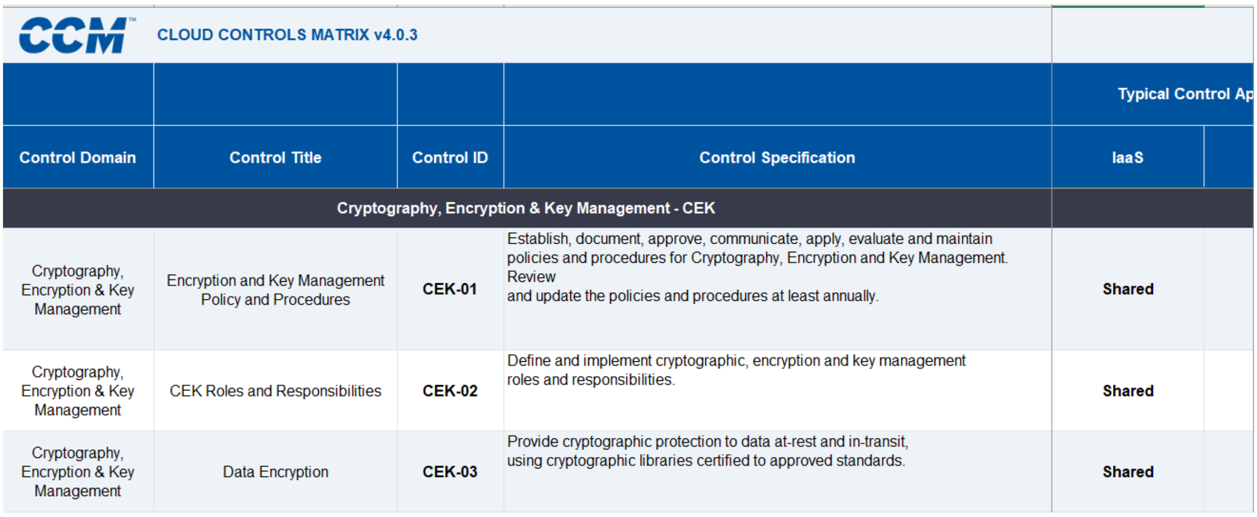
CCM™ CLOUD CONTROLS MATRIX v4.0.3

				Typical Control Ap	
Control Domain	Control Title	Control ID	Control Specification	IaaS	
Change Control and Configuration Management - CCC					
Change Control and Configuration Management	Change Management Policy and Procedures	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Shared	
Change Control and Configuration Management	Quality Testing	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	CSP-Owned	
Universal Endpoint Management	Storage Encryption	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	CSC-Owned	C
Universal Endpoint Management	Anti-Malware Detection and Prevention	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	CSC-Owned	C
Universal Endpoint Management	Software Firewall	UEM-10	Configure managed endpoints with properly configured software firewalls.	CSC-Owned	C
Universal Endpoint Management	Data Loss Prevention	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	CSC-Owned	C
Universal Endpoint			Enable remote geo-location capabilities for all managed mobile endpoints.		

Выбор масштаба. Щелкните, чтобы открыть диалоговое окно "Масшта

Figure 1.13 - CCC management matrix

Because metrics describe the measurement of security attributes in an information system, it is tempting to describe them with a detailed technical representation relying on complex XML or JSON schemas. For example, ISO/IEC 19086 proposes a machine-readable model for metrics that attempts to describe every nuance of a metric. This approach favors interoperability and reproducibility. The downside of this approach is that it limits the scope of the metrics to organizations who have the precise technical capability or tools to implement the requirements of the metric. Today, it is unclear whether the industry is ready to take this road. In this work, we take a simpler approach and focus on the definition of metrics independent of their technical representation. We want to get the feedback of the community on the value of metrics rather than their format, which could be the focus of later attention if necessary.



CLOUD CONTROLS MATRIX v4.0.3

				Typical Control Ap
Control Domain	Control Title	Control ID	Control Specification	IaaS
Cryptography, Encryption & Key Management - CEK				
Cryptography, Encryption & Key Management	Encryption and Key Management Policy and Procedures	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Shared
Cryptography, Encryption & Key Management	CEK Roles and Responsibilities	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	Shared
Cryptography, Encryption & Key Management	Data Encryption	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Shared

Figure 1.14 - Analysis of data flow in visa service using CCM

A primary security control in the CSA CCMv4 can be related to the defined metric. Implementing the metric should provide measures that can be used to partially or fully support the corresponding security control. The reference to a CSA CCM control is somewhat arbitrary, because in some cases a metric is applicable to more than one security control. However, a reference to a CCM control is useful to show that the metrics are anchored in existing security practices and it provides a way to broadly identify what is achieved in terms of security.

The description of the primary control ID from CSA CCMv4 to help the reader. A list of all other CCMv4 controls that are related to the metric in regard to the primary control already described. A metric may be related to a control in at least two ways:

- The metric may provide assurance regarding the effectiveness more than one CCMv4 control.
- The metric may be based on the assumption that other CCMv4 controls are in place because these other controls appear as necessary conditions for the correct implementation of the metric. As a consequence of the shortcomings of traditional assurance tools, organizations who want continuous assurance must reconsider their approach to security assessments. For continuous assurance, manual assessments must be traded for automated measurements, which largely leave humans out of the loop. Instead of assessing controls directly, tools are used to measure the security attributes of an information system and determine whether controls are effective in place.

For example, consider the Supply Chain Management, Transparency, and Accountability domain of CCMv4, which contains 14 control objectives. Taken together, the goal of these control objectives is to ensure that adequate tools, policies, and procedures are in place to establish, document, approve, communicate, apply, evaluate, and maintain the supply chain of CSP products and services. Notably, evaluating compliance to these control objectives requires reviewing documents, tools, processes, and governance. This kind of work is largely manual and will be done every few months. This approach fails to keep up with the changing supply chain evolutions and risks associated with fast-paced product development. Many organizations mitigate the risks by having specific technical processes in place, some of which can be automatically and regularly measured once the right tools are in place. For example:

- Maintaining an adequate inventory of supply chain relationships and automatically scanning for production packages and reconciling them with the inventory every two weeks.
- Monitoring ingress and exit connections daily and evaluating whether such connections are on the approved list of supply chain providers in the inventory.

These supply chain measures provide quantitative or qualitative values that can be contrasted with predefined objectives set by the organization in relation to its risk appetite. An organization who can set such objectives and then provide its stakeholders with measurement results that continue to support whether these objectives are met is an organization with significant maturity and awareness. These metrics also surface the interdependencies across CCMv4 control domains. For example, the effective measurement of automated STA metrics depends on the implementation of appropriate Logging and Monitoring (LOG) and Datacenter Security (DCS) controls.

CHAPTER 2
ANALYSIS AND RESEARCH OF THE FLOW OF DATA AT VISA SERVICE

2.1 Physical Security

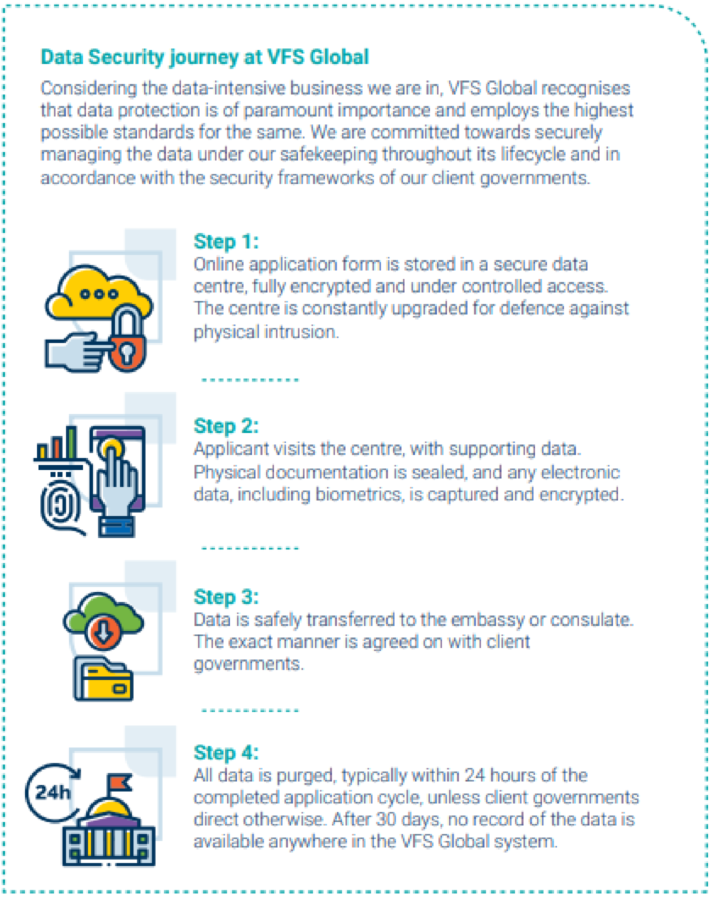
Security is a key aspect for Visa Facilitation Service Centers as it deals with different diplomatic organizations globally for visa purposes. To maintain trust, the centers ensure the highest level of data protection. It strives to make sure that its clients feel secure in all of its visa application centers. They are sealed with alarms and SMS alerts, which may automatically allow vehicles to speed stop or deviate from their specified path.

2.2 Data Protection

Visa Facilitation Service high standards of data are essential to the business model. The visa service involves scanning large amount of personal data. For security, it activates data processing. It makes the service reliable. When the paper works of clients are completed, the system purges the personal data then terminate all the applicant's information within hours of receiving it. The center makes sure that the framework of the organization works securely.

Figure 2.1- Information Security Management System

Recent outer and inner surveys conducted by visa services have identified Data Protection the most important area for the all customers. These outcomes are confirmed by available surveys, as customers need to be informed that the Visa Application Center is sure of the safekeeping of client's information. This is assured by the robust Data Protection framework.



Data Security journey at VFS Global

Considering the data-intensive business we are in, VFS Global recognises that data protection is of paramount importance and employs the highest possible standards for the same. We are committed towards securely managing the data under our safekeeping throughout its lifecycle and in accordance with the security frameworks of our client governments.

Step 1: Online application form is stored in a secure data centre, fully encrypted and under controlled access. The centre is constantly upgraded for defence against physical intrusion.

Step 2: Applicant visits the centre, with supporting data. Physical documentation is sealed, and any electronic data, including biometrics, is captured and encrypted.

Step 3: Data is safely transferred to the embassy or consulate. The exact manner is agreed on with client governments.

Step 4: All data is purged, typically within 24 hours of the completed application cycle, unless client governments direct otherwise. After 30 days, no record of the data is available anywhere in the VFS Global system.

Figure 2.2 - Data Security Journey System

An important issue of Information Security underlines the protection framework. It forms a private management System. The GDPR Regulation is most strict in the world and adheres in 144 countries. This includes diverse guards in the infrastructure of virtual systems. It also applies defense in depth model that provides defensive security mechanisms. Visa Facilitation Service does not retain applicant data longer than needed to. The information is acquired at Visa centers then sent to the diplomatic organization. The data is then erased from the initial system.

2.3 Process Excellence

The electronic visa helps in deducing client struggles through an online process thereby putting a halt to risks. In order to render a seamless service to clients, visa service introduced the following:

a. Filling the form telephone

b. Digital Application

c. Payment Online

d. Checking of document digitally

e. Contact center technology

f. Chat box

g. Click Call

h. IVR Enhancing

i. web forms

The center uses framework strategy. Visa Facilitation Service has been assisted by people capability Model to achieve business objectives. The main purpose of the work is strategic Planning. Visa service improves customer experiences.

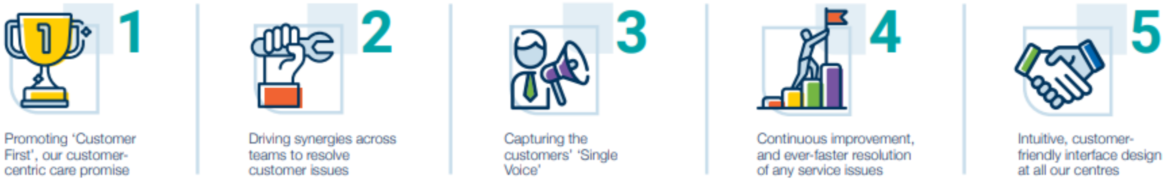
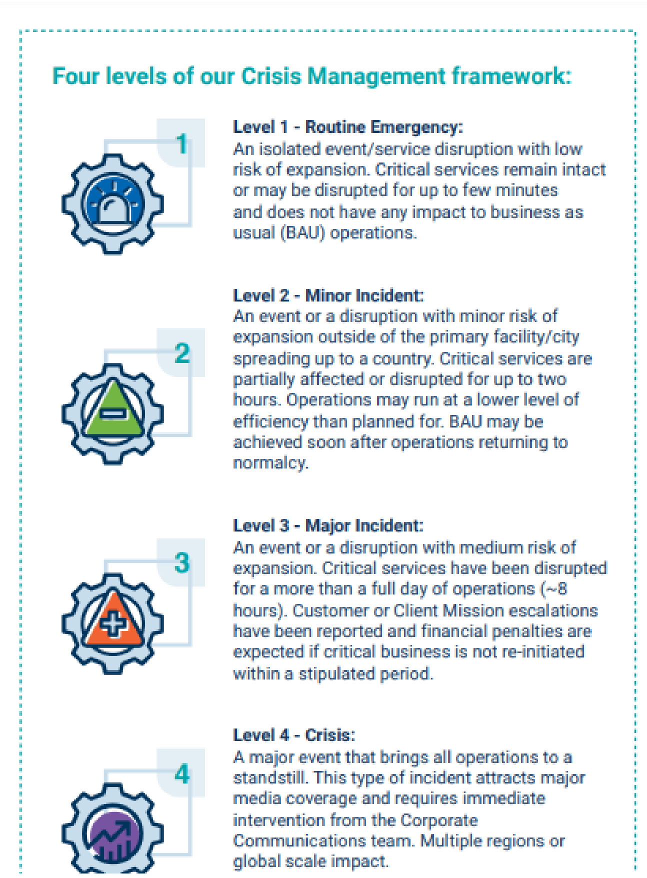

1
Promoting 'Customer First', our customer-centric care promise
2
Driving synergies across teams to resolve customer issues
3
Capturing the customers' 'Single Voice'
4
Continuous improvement, and ever-faster resolution of any service issues
5
Intuitive, customer-friendly interface design at all our centres

Figure 2.3 - Process Excellence

2.4 Business Continuity

Business Continuity Plan is set to shield troublesome business processes. At a meticulous stage, incident committee solutions help other partnered organization avoid major challenges. The resilient Center helps in the evolving incidents that would transform into a potential business continuity situation. It is what guarantees a long relation between governments and visa service providers.



Four levels of our Crisis Management framework:

1

Level 1 - Routine Emergency:
An isolated event/service disruption with low risk of expansion. Critical services remain intact or may be disrupted for up to few minutes and does not have any impact to business as usual (BAU) operations.

2

Level 2 - Minor Incident:
An event or a disruption with minor risk of expansion outside of the primary facility/city spreading up to a country. Critical services are partially affected or disrupted for up to two hours. Operations may run at a lower level of efficiency than planned for. BAU may be achieved soon after operations returning to normalcy.

3

Level 3 - Major Incident:
An event or a disruption with medium risk of expansion. Critical services have been disrupted for a more than a full day of operations (~8 hours). Customer or Client Mission escalations have been reported and financial penalties are expected if critical business is not re-initiated within a stipulated period.

4

Level 4 - Crisis:
A major event that brings all operations to a standstill. This type of incident attracts major media coverage and requires immediate intervention from the Corporate Communications team. Multiple regions or global scale impact.

Figure 2.4- Four levels of our Crisis Management framework

2.5 Security Integration

It designs systems that regulates the pending infrastructure and replace them with the latest and tech products. The solutions are always flexible and scalable. It arranges the system to optimize the workplace safety and environment. Visa services are ought to use infrastructure for increase in efficiency.

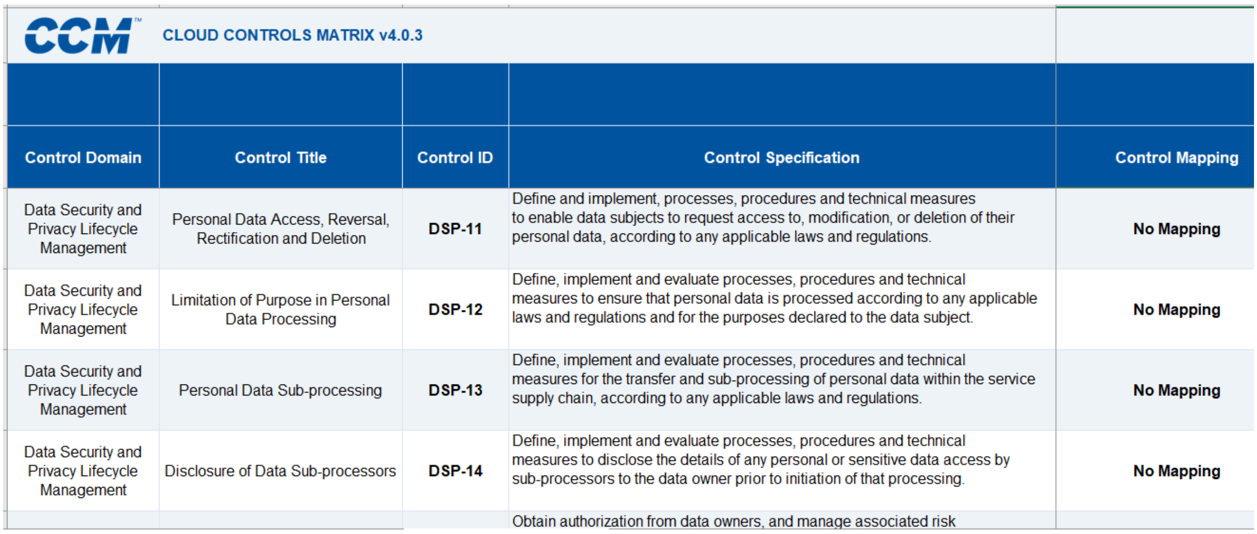
2.6 Audit Security in visa service

The metrics presented in this document are not designed to be a one-size-fits-all. Some metrics might be ignored if the organization uses the proposed metrics in a different way. Three main considerations will drive an organization to use a metric namely:

- Risk management priorities;

- Maturity; and
- Transparency.

It makes sense to focus on the most critical risks when seeking continuous assurance. An organization can choose to start with a few of metrics that target the risks. An example would be an organization that uses multiple cloud services from different vendors. It makes sense for them to focus on supply chain metrics. Metrics related to cryptography and key management are what an organization that offers health data storage might focus. A critical security attribute will likely be measured more frequently in the implementation of a metric than in the selection of the metric.



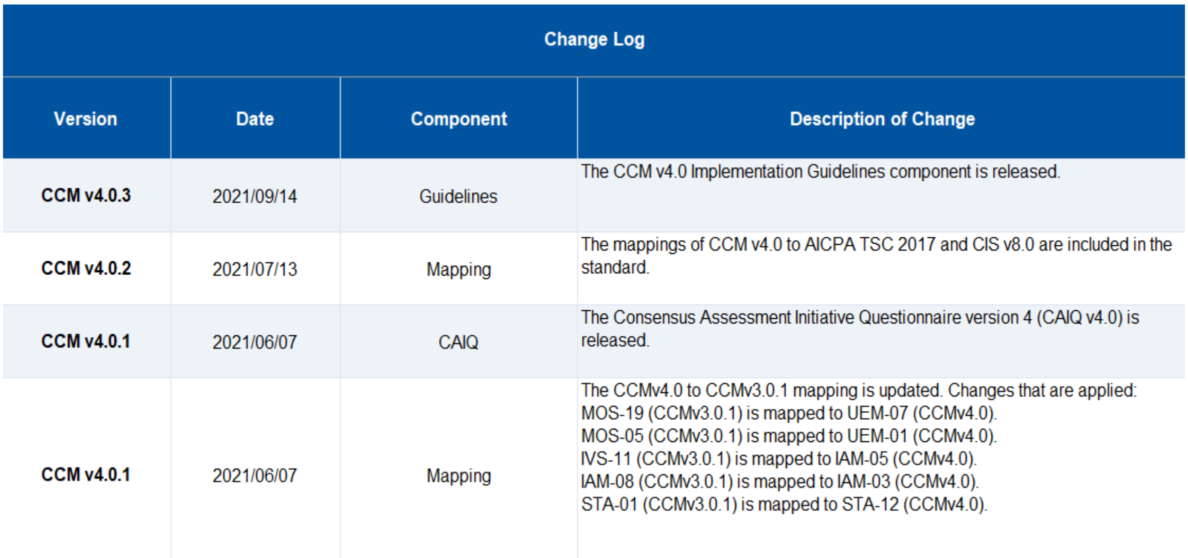
CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Control Mapping
Data Security and Privacy Lifecycle Management	Personal Data Access, Reversal, Rectification and Deletion	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	No Mapping
Data Security and Privacy Lifecycle Management	Limitation of Purpose in Personal Data Processing	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	No Mapping
Data Security and Privacy Lifecycle Management	Personal Data Sub-processing	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	No Mapping
Data Security and Privacy Lifecycle Management	Disclosure of Data Sub-processors	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	No Mapping
			Obtain authorization from data owners, and manage associated risk	

Figure 2.5- CCM mapping

Not all organizations have the level of maturity that is reflected by the existence of such tools. The selection of metrics is limited by maturity. It is possible for organizations to review these metrics as guidance for the development of their security monitoring strategy with a goal of increasing their capabilities over time. There are different levels of flexibility in the metrics of the catalog, some of which are policy dependent. Organizations with less mature policies can still achieve good results with policy dependent metrics. An organization implementing a continuous auditing program can use the catalog presented in this document to support many tasks such as:

- Measurement results should be associated with objectives that should be achieved.
- Stakeholders should be informed if the objectives are met.



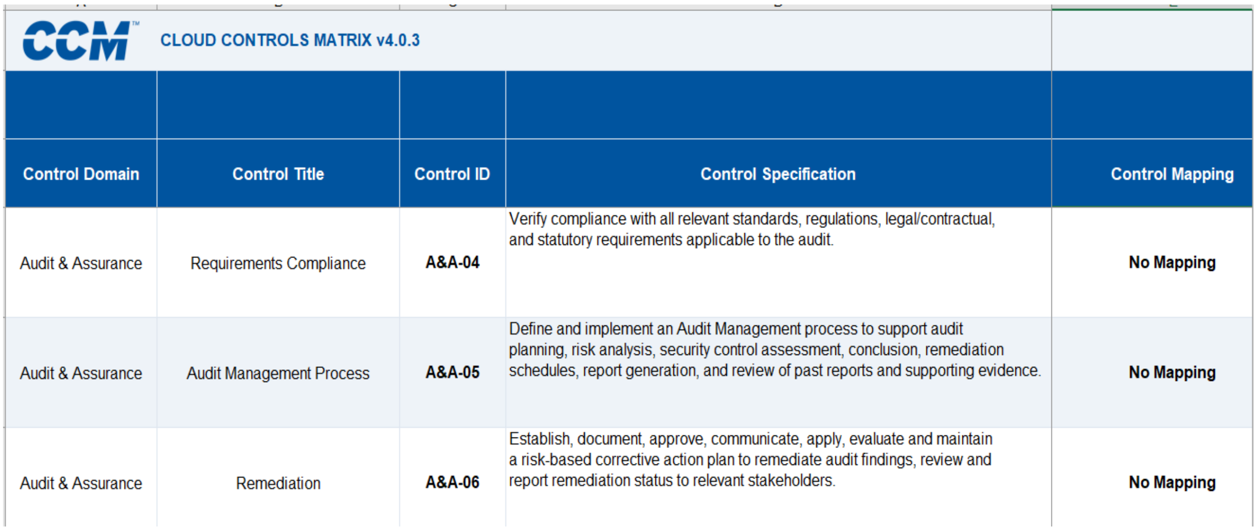
Change Log			
Version	**Date**	**Component**	**Description of Change**
CCM v4.0.3	2021/09/14	Guidelines	The CCM v4.0 Implementation Guidelines component is released.
CCM v4.0.2	2021/07/13	Mapping	The mappings of CCM v4.0 to AICPA TSC 2017 and CIS v8.0 are included in the standard.
CCM v4.0.1	2021/06/07	CAIQ	The Consensus Assessment Initiative Questionnaire version 4 (CAIQ v4.0) is released.
CCM v4.0.1	2021/06/07	Mapping	The CCMv4.0 to CCMv3.0.1 mapping is updated. Changes that are applied: MOS-19 (CCMv3.0.1) is mapped to UEM-07 (CCMv4.0). MOS-05 (CCMv3.0.1) is mapped to UEM-01 (CCMv4.0). IVS-11 (CCMv3.0.1) is mapped to IAM-05 (CCMv4.0). IAM-08 (CCMv3.0.1) is mapped to IAM-03 (CCMv4.0). STA-01 (CCMv3.0.1) is mapped to STA-12 (CCMv4.0).

Figure 2.6 - Cloud control matrix v4.0.3

- Identifying security attributes of the information system that can be measured in an automated way according to selected metrics, with measurement results providing a valid indication that certain security controls are in place.
- Frequency of measurement for each attribute is determined by feasibility, cost and risk levels.

2.7.1 Control Mapping

The mappings between standards and control sets relevant to cloud computing is found in column. The indication, of which control is in the target standard, corresponds to the CCM control.



CCM™ CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Control Mapping
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**
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**
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 report remediation status to relevant stakeholders.	**No Mapping**

Figure 2.7 - CCM mapping

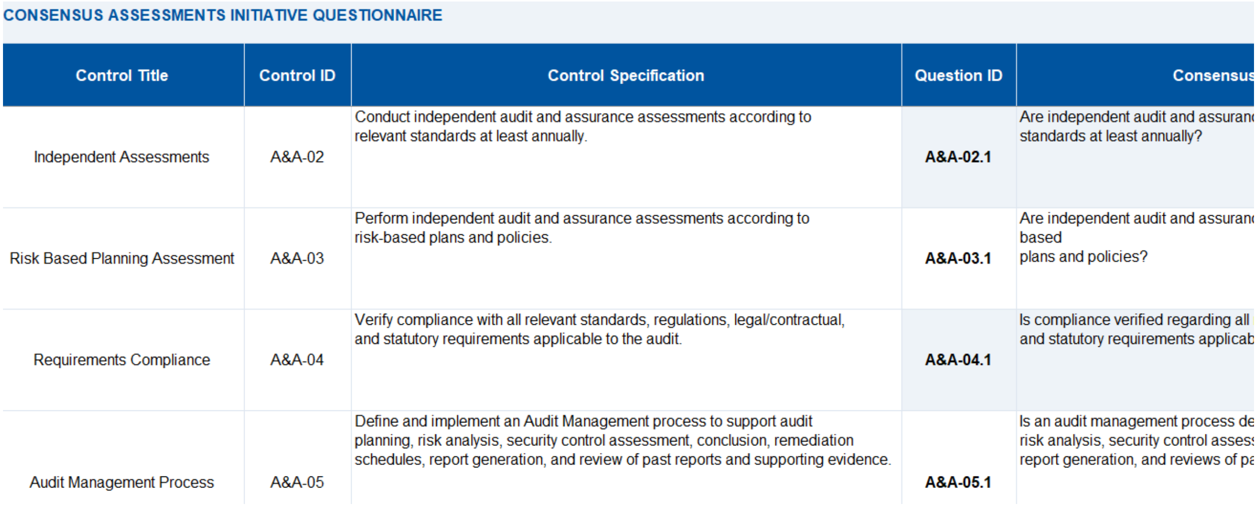
2.7.2 Gap level

The level of gap a control in the target standard is different from the level of gap a control in the CCM control. The gap levels used are:

• No Gap: In case of full correspondence.

• Partial Gap: If the control in the target standard does not fully satisfy the corresponding control’s requirements.

• Full Gap: There is a full gap if there is no control in the target standard.



CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

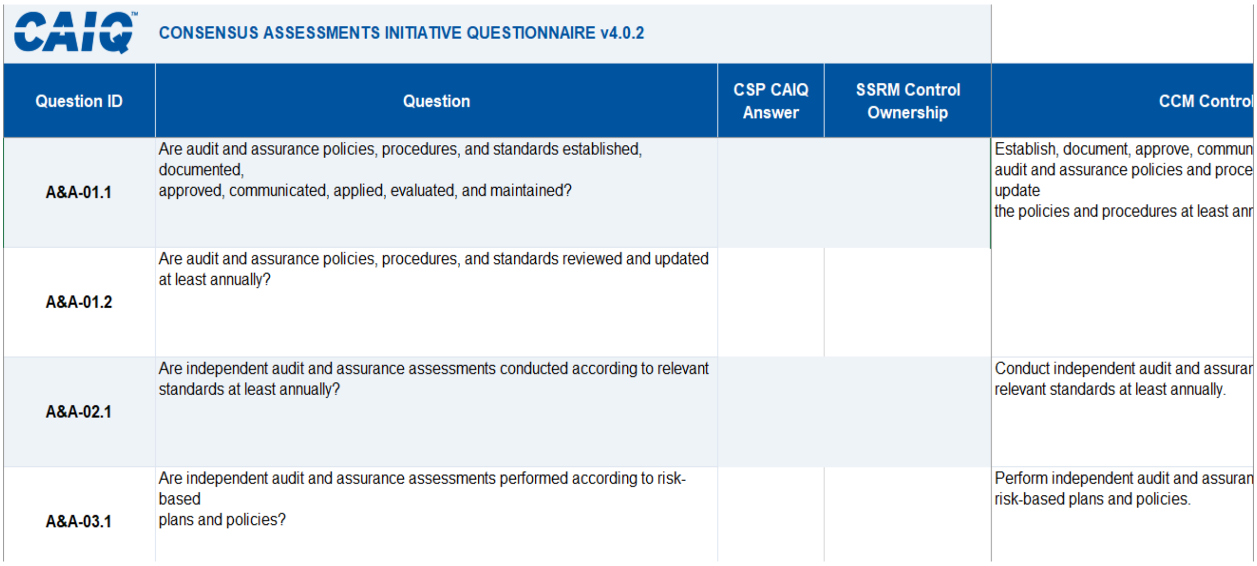
Control Title	Control ID	Control Specification	Question ID	Consensus
Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	**A&A-02.1**	Are independent audit and assuranc standards at least annually?
Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	**A&A-03.1**	Are independent audit and assuranc based plans and policies?
Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	**A&A-04.1**	Is compliance verified regarding all and statutory requirements applicab
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.	**A&A-05.1**	Is an audit management process de risk analysis, security control assess report generation, and reviews of pa

Figure 2.8- Consensus Assessments Initiative Questionnaire

2.7.3 Consensus Assessments Initiative Questionnaire

The questionnaire associated with CCM V4 controls is called CAIQ. The CAIQ comprises of 261 questions enclosed in the 17 domains of the CCM. Each question is done in the following way:

- Question ID: the questions identifier.
- Question: the description of the question.



CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CCM Control
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?			Establish, document, approve, commun audit and assurance policies and proce update the policies and procedures at least anr
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?			
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?			Conduct independent audit and assurar relevant standards at least annually.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?			Perform independent audit and assuran risk-based plans and policies.

Figure 2.9 - CSP CAIQ Answer

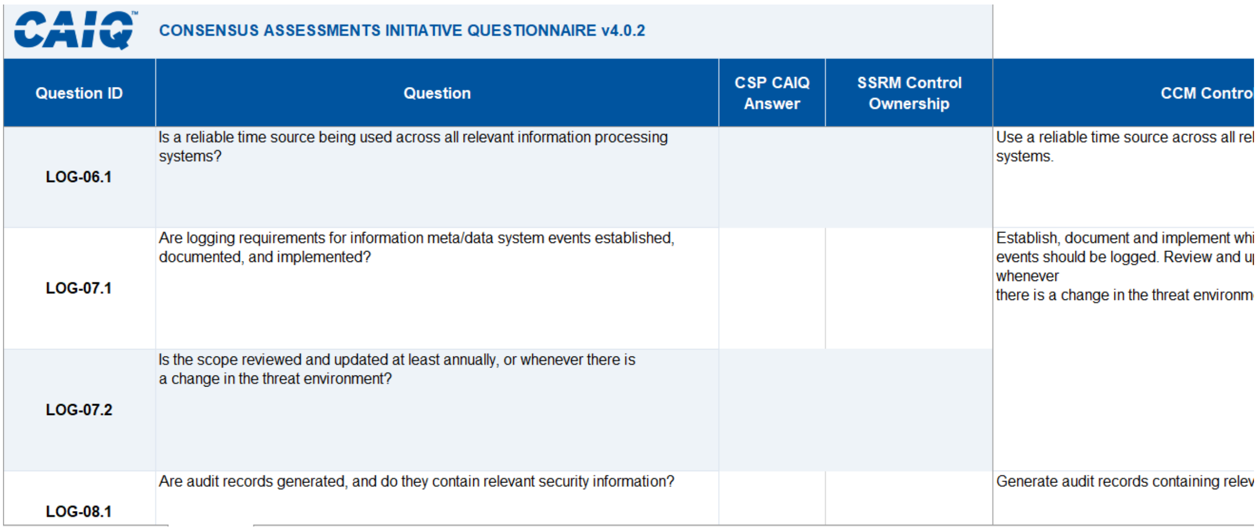
2.7.4 CSP CAIQ Answer

The Cloud Service Provider has to respond with “yes”/” no”/” n/a” next to the assessment question, and for the portion of the CCM control specification they are accountable for implementing.

Meaning of possible replies:

- “yes”: The portion of the CCM control requirement corresponding to the assessment question is met.
- “no”: The portion of the CCM control requirement corresponding to the assessment question is not met.
- “n/a”: The question does not apply to the assessment of the cloud service.

A “yes” answer shows that the portion of the control in question is implemented. The CSP displays the responsible and accountable parties and elaborates on the implementation “how-to” per relevant party CSP or CSC.



CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CCM Contro
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?			Use a reliable time source across all rel systems.
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?			Establish, document and implement whi events should be logged. Review and u whenever there is a change in the threat environm
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?			
LOG-08.1	Are audit records generated, and do they contain relevant security information?			Generate audit records containing relev

Figure 2.10 - CAIQ Answer

A "no" answer shows that the portion of the control in question is not implemented while in scope of the assessment. The CSP has to assign the responsibility of the control to the significant party under column SSRM control ownership and elaborate on the "why" and "what" has to be done for its implementation by that party.

An "n/a" answer explains that the section of the control in question is out of scope. The SSRM control ownership column is to be left blank and the CSP may explain why it is the case. Shared Security Responsibility Model Control ownership is the control applicability and ownership of the service that is identified by the CSP control responses namely:

• CSP-owned: The CSP is responsible and accountable for the CCM control.

• CSC-owned: The Cloud Service Customer is responsible and accountable for the CCM control implementation.

• Third-party outsourced the third party CSP in the supply chain is accredited for CCM control implementation while the CSP is fully accountable.

• Shared CSP and CSC: The CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is distributed between CSP and the third party but the CSP remains fully reliable.

CHAPTER 3
IMPLEMENTATION OF THE INFRASTRUCTURE FOR SECURING DATA AT VISA SERVICES

3.1 Visa Process Infrastructure System

Simplifying Visa Processing Using Excelanto (ERP) Software: This software is designed to accommodate the operation of visa processing. By means of the said software, visa service creates a process that limits strenuous issuing of visas. Time is essential and with the help of the rapid function of the software, clients have no trouble having to wait too long for their processed application. Below does the software provide the two kinds of interfaces namely:

1. Interface of Customers, which accepts request to keep track of the quantity of visas.
2. Interface of Administrative boards which processes where visa requests are conducted.

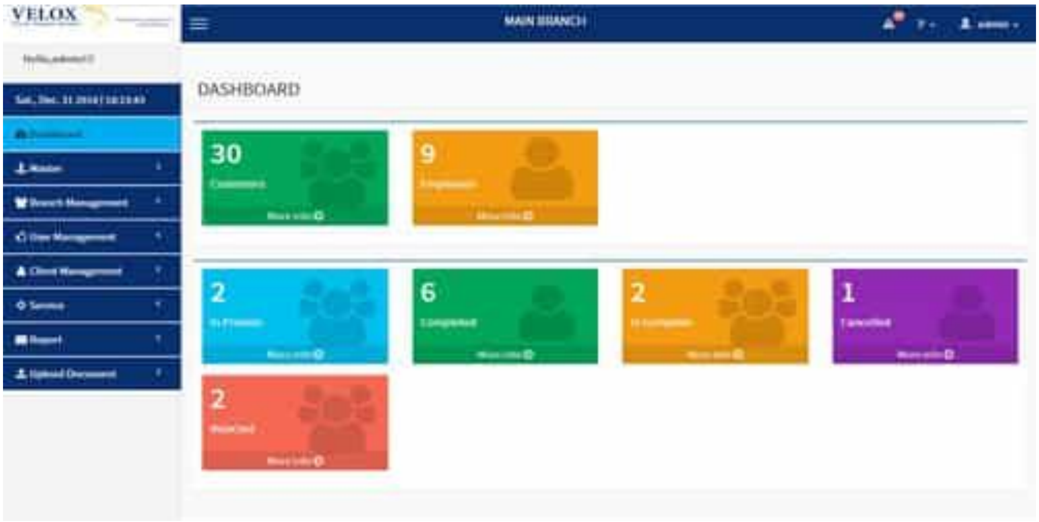
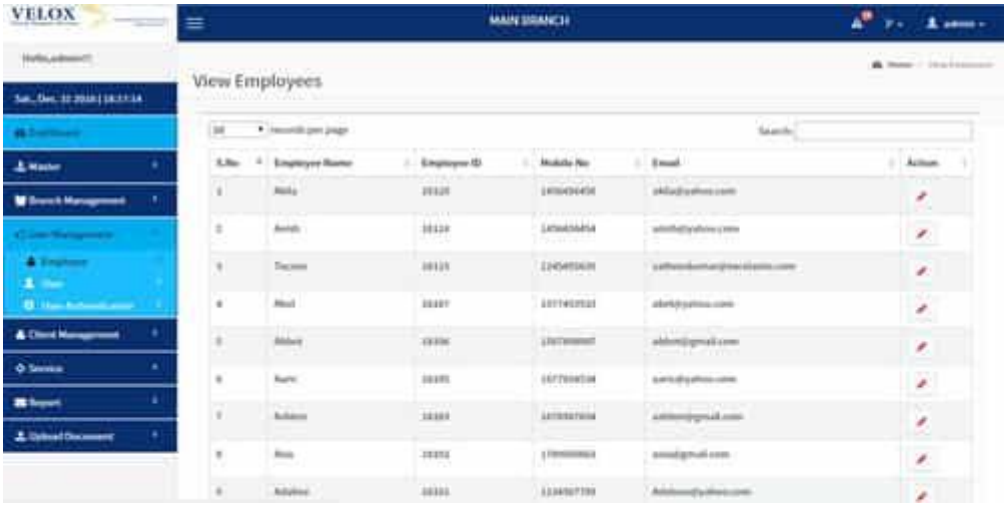


Figure 3.1- Main Branch of visa processing system

3.2 Visa Processing management System Features

This allows the flow of data smoothly through the system for visa purposes. Then it automatically sustains insights for visa details. Someone cannot allow rights to another person enabling him or her to have access to personal data. Only authorized administrative personnel who has absolute access to the system.



VELOX

MAIN BRANCH

admin

Hello, admin!!

Dashboard

Master

Branch Management

User Management

Employee

User

Client Management

Service

Report

Upload Document

View Employees

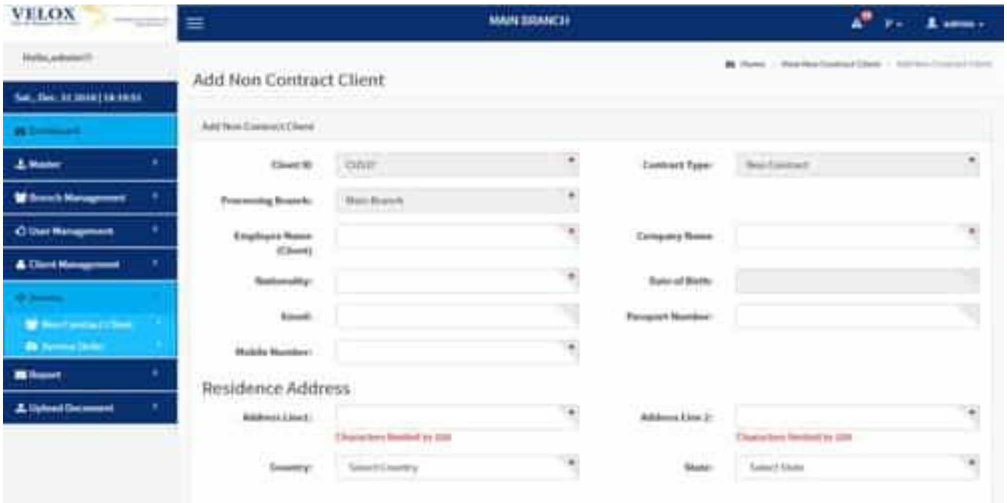
10 records per page

Search:

S.No	Employee Name	Employee ID	Mobile No	Email	Action
1	[illegible]	[illegible]	[illegible]	[illegible]	
2	[illegible]	[illegible]	[illegible]	[illegible]	
3	[illegible]	[illegible]	[illegible]	[illegible]	
4	[illegible]	[illegible]	[illegible]	[illegible]	
5	[illegible]	[illegible]	[illegible]	[illegible]	
6	[illegible]	[illegible]	[illegible]	[illegible]	
7	[illegible]	[illegible]	[illegible]	[illegible]	
8	[illegible]	[illegible]	[illegible]	[illegible]	
9	[illegible]	[illegible]	[illegible]	[illegible]	

Figure 3.2- Visa facilitation of employees

This software is designed for business to customer and business-to-business processing documents. Interested applicants may start the process online by inserting his/her data while the backend proceeds to commence. Through this means, one can apply and track his or her application virtually.



VELOX

MAIN BRANCH

admin

Hello, admin!!

Dashboard

Master

Branch Management

User Management

Client Management

Service

Report

Upload Document

Add Non Contract Client

Add Non Contract Client

Client ID:
Contract Type: Non Contract

Processing Branch: Main Branch

Employee Name (Client):
Company Name:

Nationality:
Date of Birth:

Email:
Passport Number:

Mobile Number:

Residence Address

Address Line1:
Address Line 2:

Characters limited to 100

Country: Select Country
State: Select State

Figure 3.3- Contact Client processing system

The software is accepting enormous requests enabling one to insert all his/her details in an excelan. Using paperless service, the visa process is faster and the response time is not lengthy. A person’s information is acquired by the software and kept safely for future use.

3.3 Privacy and data protection:

Countries consult their own codes as well as international agreements to ensure they have authority to share traveler’s data. State policies on the use of passenger data differ considerably.

It is interesting for example, that the implementing legislation for the US trusted traveler program which appears to prevent individual passengers from demanding access to their personal data held in official files. In contrast, the proposed EU program observes the data access protections enshrined in a number of EU codes including the EU Charter of Fundamental Rights. Regardless of the jurisdiction, strict standards will have to be adopted for recording, accessing, storage and disposing of personal data. It is also important to be proactive from a public awareness standpoint, reassuring travelers about the protections in place to prevent misuse or appropriation of their personal data or biometric information.

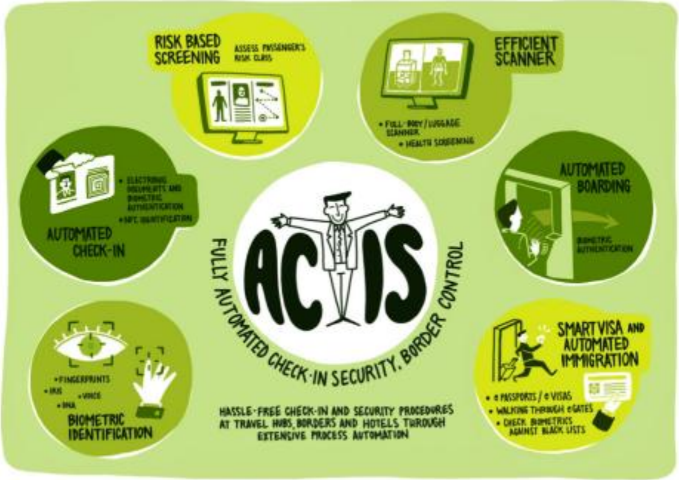

RISK BASED SCREENING
ASSESS PASSENGER'S RISK CLASS
EFFICIENT SCANNER
• FULL-BODY / LUGGAGE SCANNER
• HEALTH SCREENING
• ELECTRONIC DOCUMENTS AND BIOMETRIC AUTHENTICATION
• NFC IDENTIFICATION
AUTOMATED CHECK-IN
AUTOMATED BOARDING
BIOMETRIC AUTHENTICATION
ACIS
FULLY AUTOMATED CHECK-IN SECURITY, BORDER CONTROL
• FINGERPRINTS
• IRIS
• VOICE
• DNA
BIOMETRIC IDENTIFICATION
HASSLE-FREE CHECK-IN AND SECURITY PROCEDURES AT TRAVEL HUBS, BORDERS AND HOTELS THROUGH EXTENSIVE PROCESS AUTOMATION
SMARTVISA AND AUTOMATED IMMIGRATION
• e PASSPORTS / e VISAS
• WALKING THROUGH eGATES
• CHECK BIOMETRICS AGAINST BLACK LISTS

Figure 3.4 - Automated check-in security

3.4 Models for smart travel

Twenty-first century technology offers a variety of innovative solutions to many of the problems that frustrate travelers and restrict growth in the travel and tourism sector. For example, in 2013, the first 14 “smart access” opened in Dubai International Airport Terminal 3, which automates security checkpoints by biometric recognition. International organizations and industry associations have also taken concrete steps to improve the traveler’s experience through technological advancements. The International Air Transport Association has developed SMARTS, a concept for an airport security system that uses advanced scanning technology with eye and face recognition protocols capable of drastically changing the security of the airports.

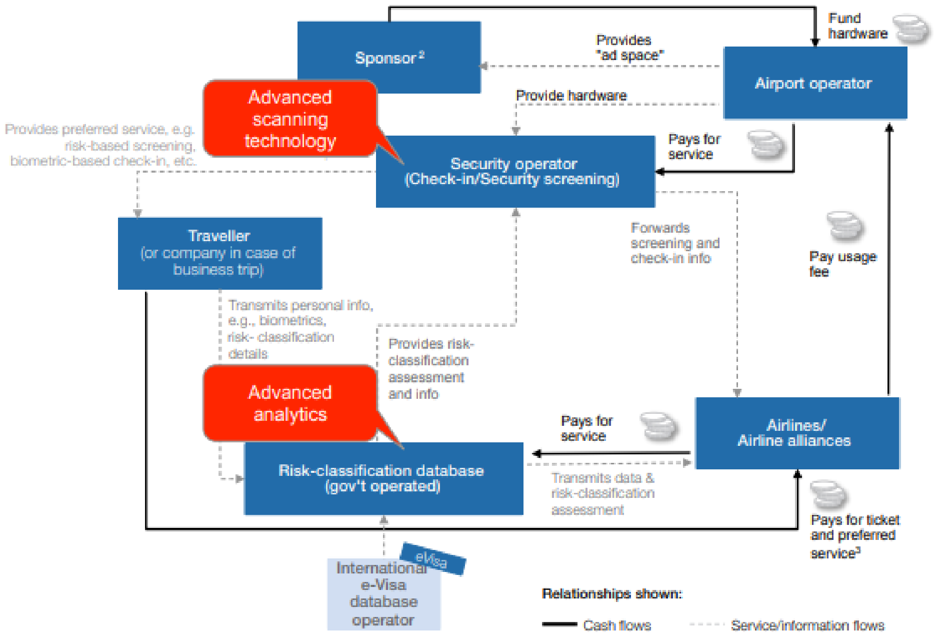

Sponsor²
Provides "ad space"
Fund hardware
Airport operator
Advanced scanning technology
Provide hardware
Provides preferred service, e.g. risk-based screening, biometric-based check-in, etc.
Security operator (Check-in/Security screening)
Pays for service
Traveller (or company in case of business trip)
Forwards screening and check-in info
Pay usage fee
Transmits personal info, e.g., biometrics, risk- classification details
Provides risk-classification assessment and info
Advanced analytics
Pays for service
Airlines/ Airline alliances
Risk-classification database (gov't operated)
Transmits data & risk-classification assessment
Pays for ticket and preferred service³
International e-Visa database operator
eVisa
Relationships shown:
Cash flows
Service/information flows

Figure 3.5 - Smart Airport System

Both of these initiatives can be found on the ICAO website. The APEC Travel Facilitation Initiative includes plans for cross-border cooperation on trusted traveler programs, the use of advanced passenger information and other travel facilitation tools. In parallel, the World Economic Forum proposes a solution that uses technology and new operational and business models to improve the visa processing and approval structures, as well as travel facilitation at immigration borders and airport security check-in.

3.5 Aspirational Smart Travel:

Under the streamlined process of Fully Automated Check-in, Security and Border Control and Smart Visa, travelers can submit and receive their visas electronically once the information has been crosschecked against the relevant databases. Visa approval would be digitally recorded and accessible by automated fingerprint or iris scanners at security checkpoints as part of a comprehensive process that includes flight check-in and registration along with security examination in one easy step. The process is described in the sidebar ACIS Solution, a traveler’s Vantage Point”.

The first component of ACIS – the review and enhancement of the current visa process can be achieved by a variety of reforms.

Full ACIS implementation of ACIS would allow travelers to submit their application and pay fees online to a visa processing service that would instantaneously check the applicant’s information against the government-run database and update the applicant’s record within the database based on the information submitted. The information would also be crosschecked against international visa databases and security organizations such as Interpol.

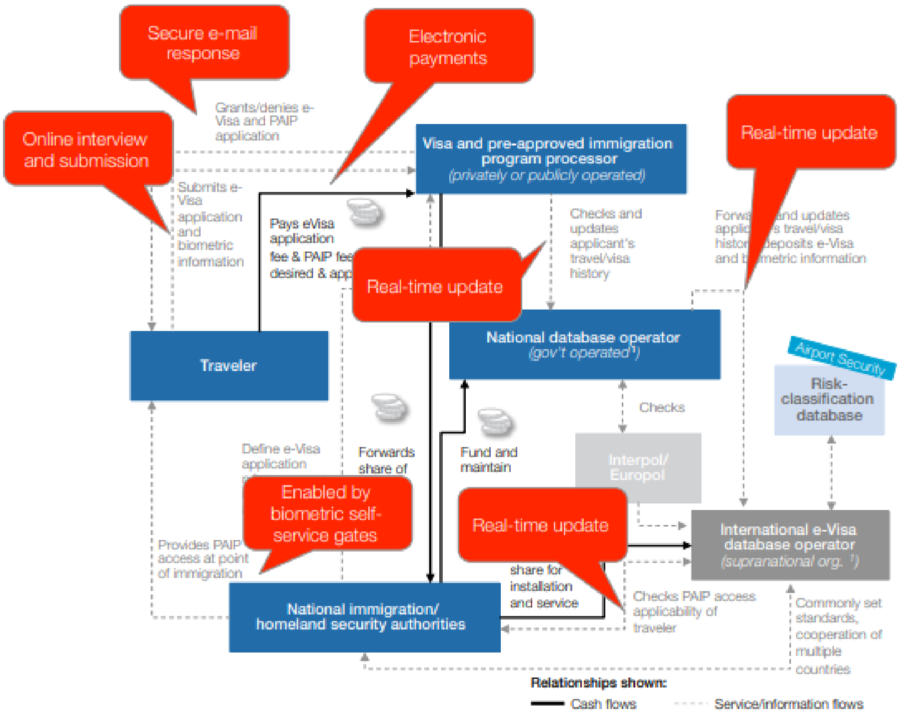

Secure e-mail response
Electronic payments
Online interview and submission
Grants/denies e-Visa and PAIP application
Visa and pre-approved immigration program processor
(privately or publicly operated)
Real-time update
Submits e-Visa application and biometric information
Pays eVisa application fee & PAIP fee desired & app
Checks and updates applicant's travel/visa history
Forwa and updates applic s travel/visa histor deposits e-Visa and b metric information
Real-time update
Traveler
National database operator
(gov't operated¹)
Airport Security
Risk-classification database
Checks
Define e-Visa application
Forwards share of
Fund and maintain
Interpol/ Europol
Enabled by biometric self-service gates
Real-time update
International e-Visa database operator
(supranational org. ¹)
Provides PAIP access at point of immigration
share for installation and service
Checks PAIP access applicability of traveler
Commonly set standards, cooperation of multiple countries
National immigration/ homeland security authorities
Relationships shown:
Cash flows
Service/information flows

Figure 3.6 - Smart Visa system

The applicant would be spared the inconvenience of travelling to a consular office, but also receive an immediate approval or rejection of the application, eliminating the uncertainty and long wait periods that deter travelers. The second component of the travel process that would be significantly changed under ACIS is the system of airport security checks. Travelers would pre-submit their information to a risk classification database, which would provide an assessment of the passenger’s risk level to the airport Figure 1: Smart Visa security operator allows risk-based screening at the airport. The security operator would send the necessary information to the appropriate airline, eliminating the need for check-in desks or long security lines once the passenger's identity was confirmed by biometric scan.

3.6 Visas and Borders: The Key for Seamless Travel

Importantly, the airport security upgrades through ACIS would operate entirely independently of a state's visa system. Nevertheless, the ACIS solution envisions the visa system feeding into the ACIS security apparatus to create an efficient, seamless experience for the traveler. The ACIS Smart Travel system would collect the traveler's information once and then redistribute it across the various agencies and checkpoints for approval and verification purposes during the trip.

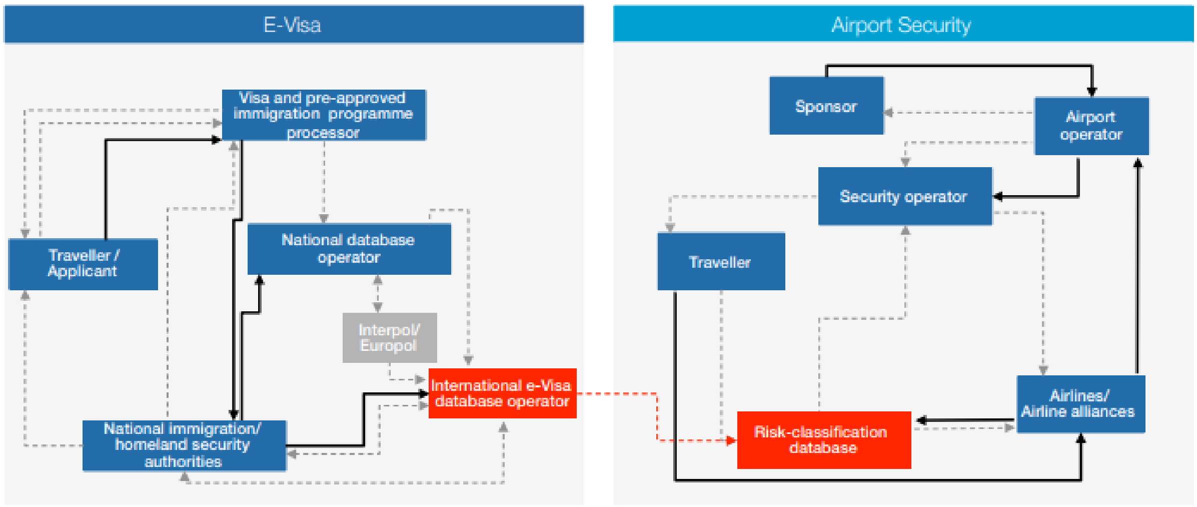

E-Visa
Visa and pre-approved immigration programme processor
Traveller / Applicant
National database operator
Interpol/ Europol
International e-Visa database operator
National immigration/ homeland security authorities
Airport Security
Sponsor
Airport operator
Security operator
Traveller
Airlines/ Airline alliances
Risk-classification database

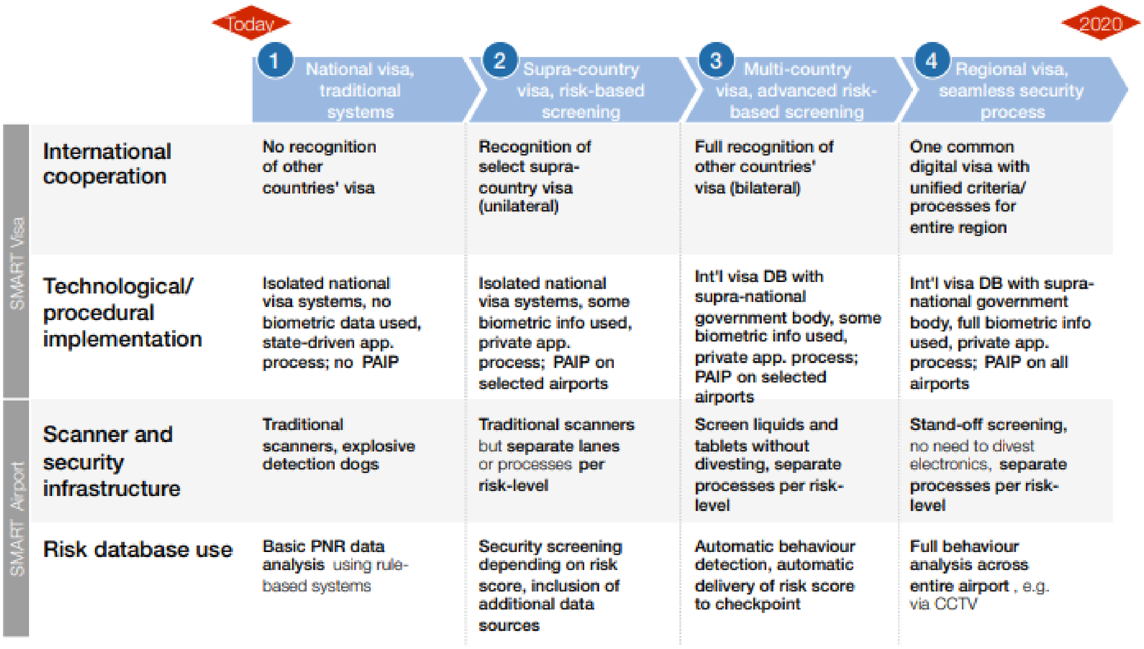
Figure 3.7- Interface between international e-visa database and Airport security

The result would be a highly efficient system that speeds up travel without needless delays or manual processing.

3.7 A Roadmap to Implementation

The components of the Smart Travel system are expected to progress through four phases of implementation. The first phase is the current environment in many countries with national visas awarded through traditional applications. In the phase, states do not recognize visas granted to visitors by neighboring countries. Visa applications do not collect biometric data; there is no communication between states on individual applications; and there are no preapproval programs. Security infrastructure is composed of conventional scanning machines and bomb-sniffing dogs, and only basic passenger name recognition analysis is conducted.

When each component has advanced to the second phase, select countries would unilaterally recognize certain supra-country visas; national visa systems would use biometric data and private application processors, and select airports would offer PAIPs. Scanning technology would not be dramatic improvement, but security lanes would be separated by passenger risk level. Additional data sources would be used to assign the risk scores to passengers for security screening purposes. By phase three, many countries would accept passengers with visas from other states, and more access would proliferate through reciprocal bilateral agreements as well as unilateral recognition. An international visa database could be created and overseen by an intergovernmental body. Use of biometric information and private visa processors would continue to increase. Scanning technology would be able to screen liquids and electronic devices without passengers need to remove them from their bags. Security monitors would use some behavior detection abilities and receive automatic delivery of passengers' risk scores after the processing of their visas.

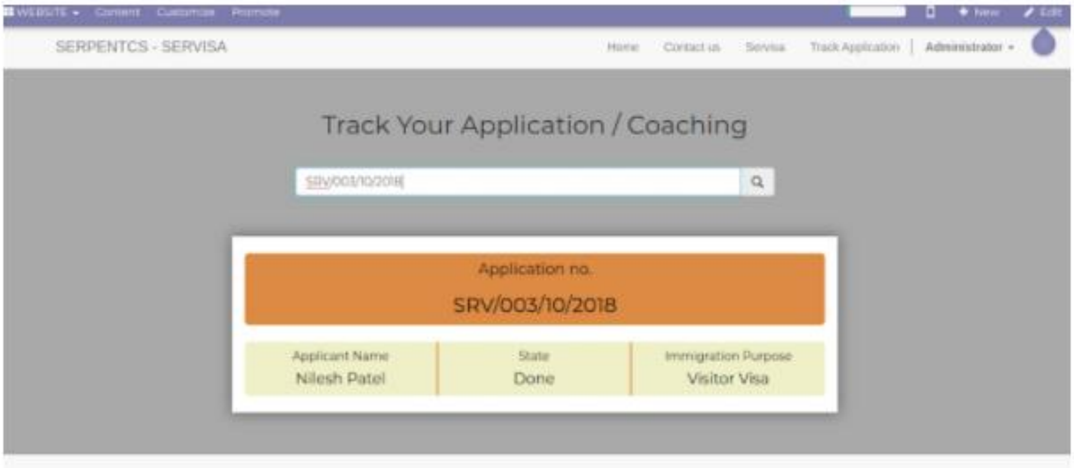


		Today			2020
		1 National visa, traditional systems	2 Supra-country visa, risk-based screening	3 Multi-country visa, advanced risk-based screening	4 Regional visa, seamless security process
SMART Visa	International cooperation	No recognition of other countries' visa	Recognition of select supra-country visa (unilateral)	Full recognition of other countries' visa (bilateral)	One common digital visa with unified criteria/ processes for entire region
	Technological/ procedural implementation	Isolated national visa systems, no biometric data used, state-driven app. process; no PAIP	Isolated national visa systems, some biometric info used, private app. process; PAIP on selected airports	Int'l visa DB with supra-national government body, some biometric info used, private app. process; PAIP on selected airports	Int'l visa DB with supra-national government body, full biometric info used, private app. process; PAIP on all airports
SMART Airport	Scanner and security infrastructure	Traditional scanners, explosive detection dogs	Traditional scanners but separate lanes or processes per risk-level	Screen liquids and tablets without divesting, separate processes per risk-level	Stand-off screening, no need to divest electronics, separate processes per risk-level
	Risk database use	Basic PNR data analysis using rule-based systems	Security screening depending on risk score, inclusion of additional data sources	Automatic behaviour detection, automatic delivery of risk score to checkpoint	Full behaviour analysis across entire airport , e.g. via CCTV

Figure 3.8 - Four Phases of the ACIS Roadmap

Finally, in phase four, the ACIS Smart Travel vision will be complete when travelers can obtain a single digital visa for each region they wish to travel. Each region will have its own application process and approval criteria common across all states within the region. All airports will have PAIPs and the private application processors will send a full array of biometric information to the international visa database, which will crosscheck the information against applications filed in other regions.

There will be no need for passengers to divest themselves of any electronics because standoff screening will be possible. Closed-circuit monitors will conduct a full behavioral analysis of all persons within every airport. SerpentCS smart tool found in Odoo v8 system rendering important traits for outlining the rights to all workers access to client's data that are handled in the system. It is a wide spread tool used by majority of the visa application centers today.



Track Your Application / Coaching

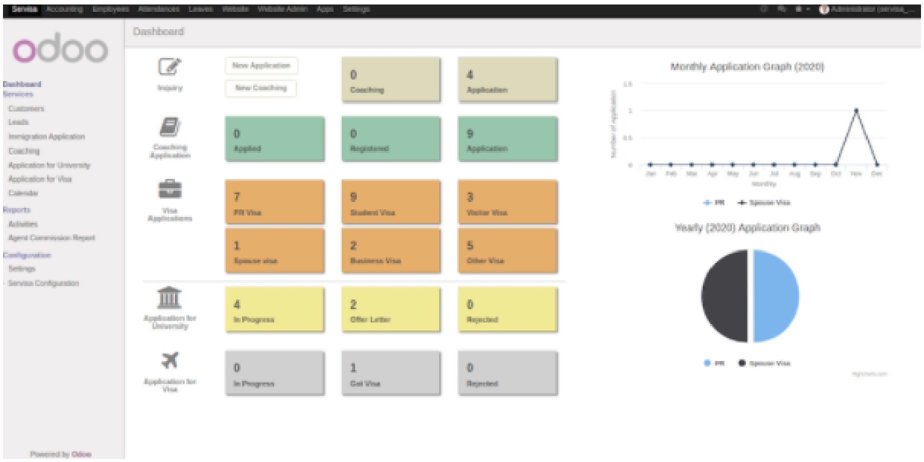
SRV/003/10/2018

Application no.
SRV/003/10/2018

Applicant Name	State	Immigration Purpose
Nilesh Patel	Done	Visitor Visa

Figure 3.9 - overview of SerpentCS Visa Application Tracking

A perfect insight is one that is expected by client when accessing the software. This provides all business flows with the assistance of modules like crm, sales, buy and inventory analysis.



Inquiry	New Application New Coaching	0 Coaching	4 Application
Coaching Application	0 Applied	0 Registered	9 Application
Visa Applications	7 PR Visa	9 Student Visa	3 Visitor Visa
	1 Spouse visa	2 Business Visa	5 Other Visa
Application for University	4 In Progress	2 Offer Letter	0 Rejected
Application for Visa	0 In Progress	1 Got Visa	0 Rejected

Figure 3.10 - Overview of smart tool in Odoo

Components in visa structured source:

- Relations of client Management.
- structuring of documents
- sorting of Time sheet
- Sales & buying of Management.
- Management Inventory
- Accounting Management.
- Management of pay roll
- Invoicing Arrangement
- Maintenance of migration status
- Marketing control
- Management of visa attendant
- Virtual visa tracking

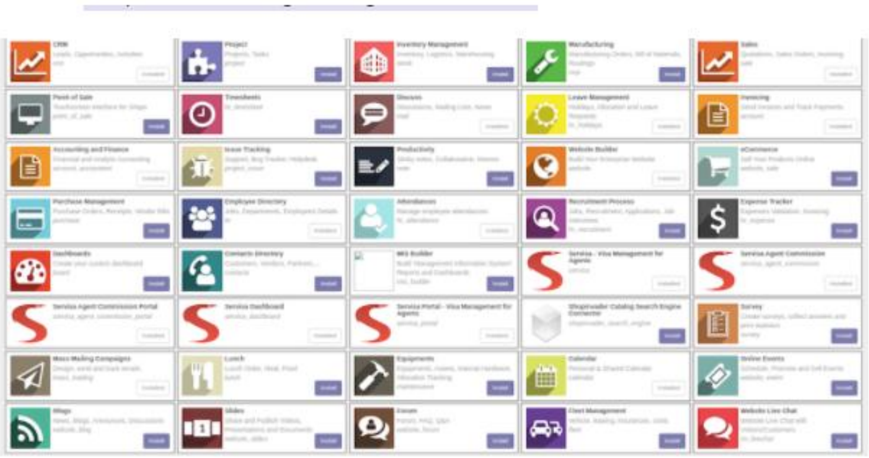
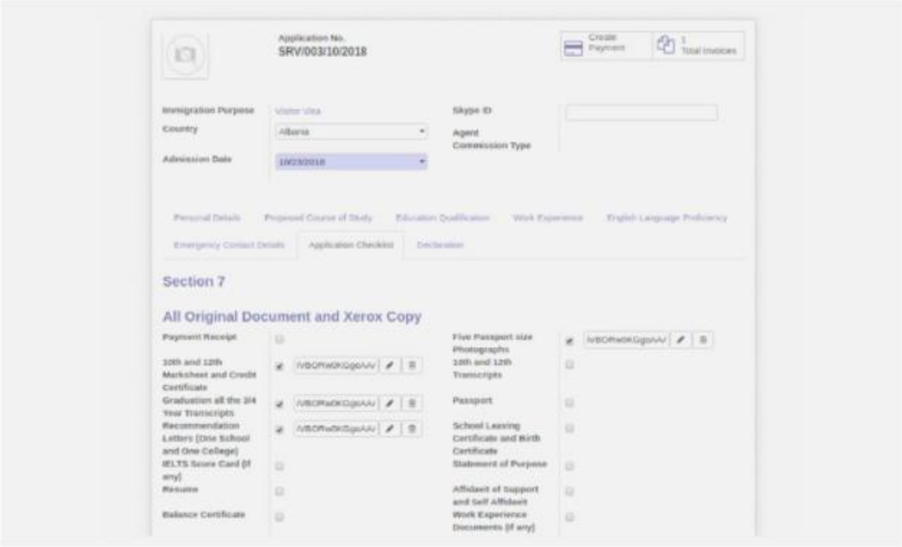


Figure 3.11 - common features used in SerpentCS

The visa management services can formulate custom travel documentations in respect to travel needs by a visible channel and innovative process. Below are common problems or errors that security agents do when clients are filling in their online visa applications.



Application No.
SRV/003/10/2018

Immigration Purpose: Visitor Visa
Country: Albania
Admission Date: 10/23/2018
Skype ID
Agent
Commission Type

Section 7

All Original Document and Xerox Copy

Payment Receipt	□	Five Passport size Photographs	☑ iVBORw0KGgoAAV
10th and 12th Marksheet and Credit Certificate	☑ iVBORw0KGgoAAV	10th and 12th Transcripts	□
Graduation all the 3/4 Year Transcripts	☑ iVBORw0KGgoAAV	Passport	□
Recommendation Letters (One School and One College)	☑ iVBORw0KGgoAAV	School Leaving Certificate and Birth Certificate	□
IELTS Score Card (if any)	□	Statement of Purpose	□
Resume	□	Affidavit of Support and Self Affidavit	□
Balance Certificate	□	Work Experience Documents (if any)	□

Figure 3.12- Visa application Template using Serpent CS

1. Unavailable access to the system “visa://IP Address/DYI3::17: PNRST”

Driver

- NI-VISA

Issue Details

I installed the necessary software and configured the hardware for PXI controller but each time I try to access any of the systems I receive the following error:

```
      Unavailable access to the system “visa://192.168.33.9/PXI2::17::PNRST”
      home level code: 2xPFFF01A6
      home title: VI_failed_NAccess
      Admittance to the remote system is not allowed. This problem is due to the
deficiency of abundant rights of the pending user system.
```

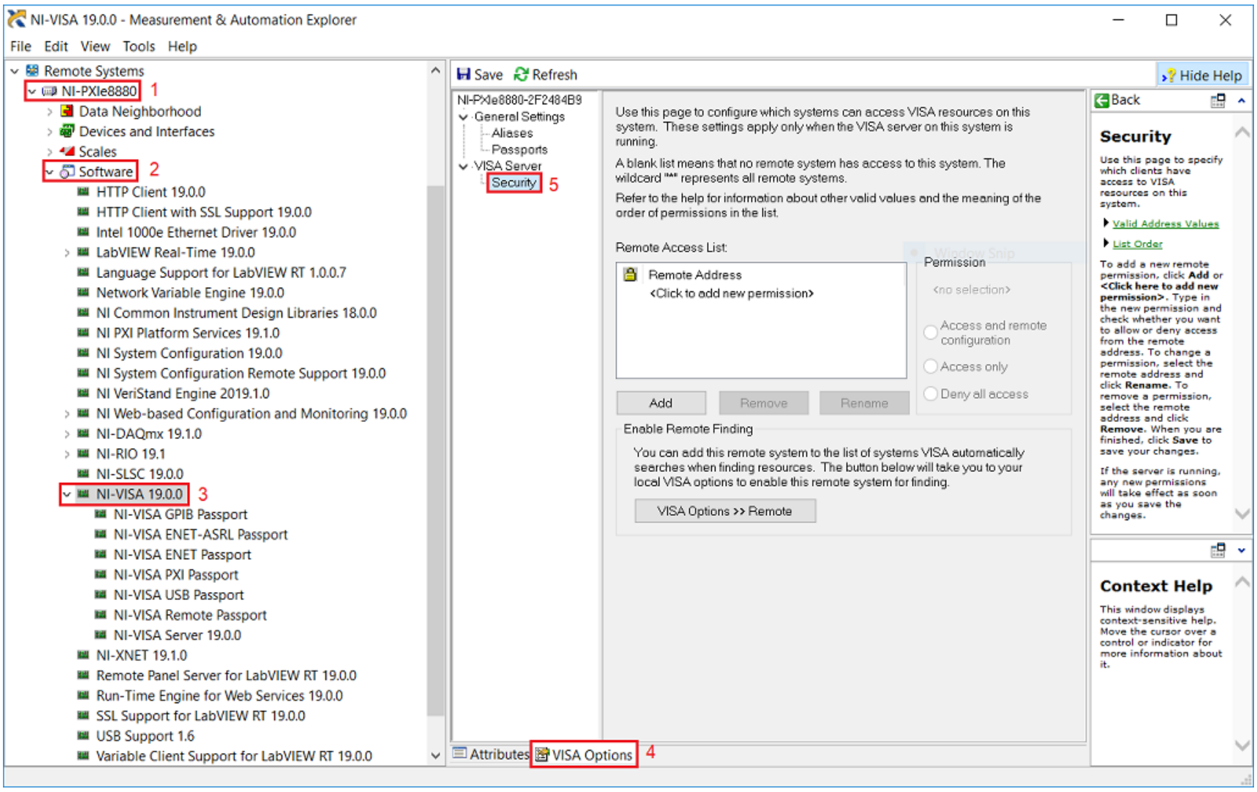
Client: What is going on and why do I get this error?

Solution

This error is due to the visa security settings. In NI MAX (Measurement and Automation Explorer), you must explicitly give permission to the host computer trying to target the PXI Controller. Follow the steps below in order to configure the visa security settings:

Open NI MAX. Navigate to Remote Systems » Your PXI Controller » Software » NI visa *x.x.*

Switch to visa Options tab. Click on Security in the main windows.


NI-VISA 19.0.0 - Measurement & Automation Explorer
File Edit View Tools Help
Remote Systems
NI-PXIe8880
1
Data Neighborhood
Devices and Interfaces
Scales
Software
2
HTTP Client 19.0.0
HTTP Client with SSL Support 19.0.0
Intel 1000e Ethernet Driver 19.0.0
LabVIEW Real-Time 19.0.0
Language Support for LabVIEW RT 1.0.0.7
Network Variable Engine 19.0.0
NI Common Instrument Design Libraries 18.0.0
NI PXI Platform Services 19.1.0
NI System Configuration 19.0.0
NI System Configuration Remote Support 19.0.0
NI VeriStand Engine 2019.1.0
NI Web-based Configuration and Monitoring 19.0.0
NI-DAQmx 19.1.0
NI-RIO 19.1
NI-SLSC 19.0.0
NI-VISA 19.0.0
3
NI-VISA GPIB Passport
NI-VISA ENET-ASRL Passport
NI-VISA ENET Passport
NI-VISA PXI Passport
NI-VISA USB Passport
NI-VISA Remote Passport
NI-VISA Server 19.0.0
NI-XNET 19.1.0
Remote Panel Server for LabVIEW RT 19.0.0
Run-Time Engine for Web Services 19.0.0
SSL Support for LabVIEW RT 19.0.0
USB Support 1.6
Variable Client Support for LabVIEW RT 19.0.0
Save
Refresh
Hide Help
NI-PXIe8880-2F2484B9
General Settings
Aliases
Passports
VISA Server
Security
5
Remote Access List
Remote Address
<Click to add new permission>
Permission
<no selection>
○ Access and remote configuration
○ Access only
○ Deny all access
Add
Remove
Rename
Enable Remote Finding
VISA Options >> Remote
Attributes
VISA Options
4
Back
Security
Valid Address Values
List Order
Context Help

Use this page to configure which systems can access VISA resources on this system. These settings apply only when the VISA server on this system is running.

A blank list means that no remote system has access to this system. The wildcard "*" represents all remote systems.

Refer to the help for information about other valid values and the meaning of the order of permissions in the list.

You can add this remote system to the list of systems VISA automatically searches when finding resources. The button below will take you to your local VISA options to enable this remote system for finding.

Use this page to specify which clients have access to VISA resources on this system.

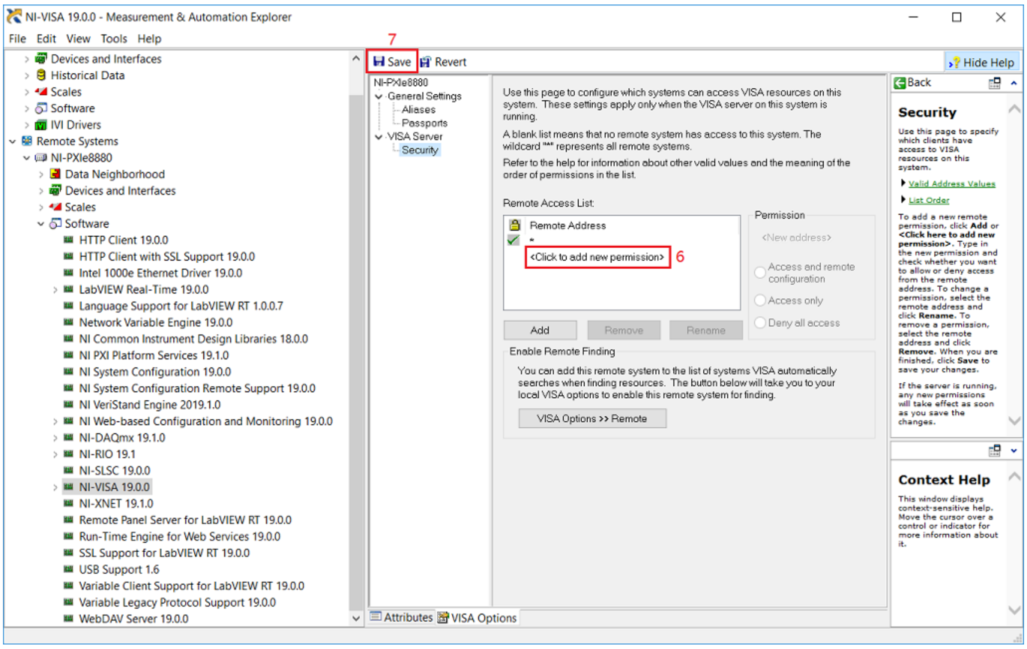
To add a new remote permission, click **Add** or **<Click here to add new permission>**. Type in the new permission and check whether you want to allow or deny access from the remote address. To change a permission, select the remote address and click **Rename**. To remove a permission, select the remote address and click **Remove**. When you are finished, click **Save** to save your changes.

If the server is running, any new permissions will take effect as soon as you save the changes.

This window displays context-sensitive help. Move the cursor over a control or indicator for more information about it.

Figure 3.13 - Measurement and Automation Explorer

Click on Click to add new permission. Enter either the IP address of the host computer or Enter * (an asterisk) to allow access to all computers on the same network. Save the settings by clicking the Save button at the top of the window and reboot the controller.


NI-VISA 19.0.0 - Measurement & Automation Explorer
File Edit View Tools Help
Devices and Interfaces
Historical Data
Scales
Software
IVI Drivers
Remote Systems
NI-PXIe8880
Data Neighborhood
Devices and Interfaces
Scales
Software
HTTP Client 19.0.0
HTTP Client with SSL Support 19.0.0
Intel 1000e Ethernet Driver 19.0.0
LabVIEW Real-Time 19.0.0
Language Support for LabVIEW RT 1.0.0.7
Network Variable Engine 19.0.0
NI Common Instrument Design Libraries 18.0.0
NI PXI Platform Services 19.1.0
NI System Configuration 19.0.0
NI System Configuration Remote Support 19.0.0
NI VeriStand Engine 2019.1.0
NI Web-based Configuration and Monitoring 19.0.0
NI-DAQmx 19.1.0
NI-RIO 19.1
NI-SLSC 19.0.0
NI-VISA 19.0.0
NI-XNET 19.1.0
Remote Panel Server for LabVIEW RT 19.0.0
Run-Time Engine for Web Services 19.0.0
SSL Support for LabVIEW RT 19.0.0
USB Support 1.6
Variable Client Support for LabVIEW RT 19.0.0
Variable Legacy Protocol Support 19.0.0
WebDAV Server 19.0.0
7
Save
Revert
Hide Help
NI-PXIe8880
General Settings
Aliases
Passports
VISA Server
Security
Remote Access List
Remote Address
*
<Click to add new permission>
6
Permission
<New address>
○ Access and remote configuration
○ Access only
○ Deny all access
Add
Remove
Rename
Enable Remote Finding
VISA Options >> Remote
Attributes
VISA Options
Back
Security
Valid Address Values
List Order
Context Help

Use this page to configure which systems can access VISA resources on this system. These settings apply only when the VISA server on this system is running.

A blank list means that no remote system has access to this system. The wildcard "*" represents all remote systems.

Refer to the help for information about other valid values and the meaning of the order of permissions in the list.

You can add this remote system to the list of systems VISA automatically searches when finding resources. The button below will take you to your local VISA options to enable this remote system for finding.

Use this page to specify which clients have access to VISA resources on this system.

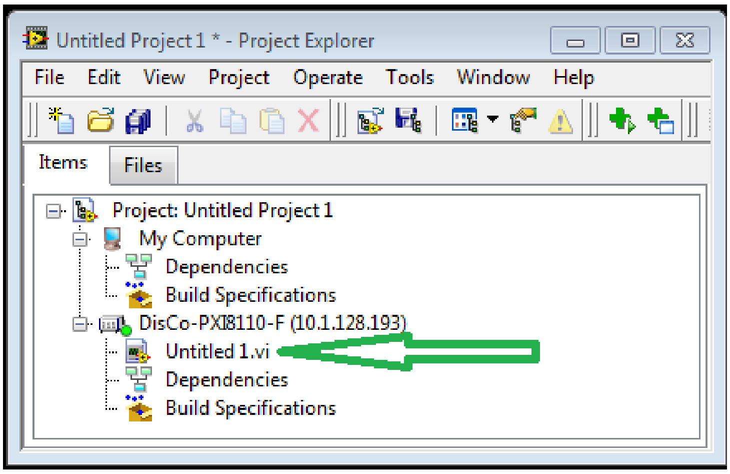
To add a new remote permission, click **Add** or **<Click here to add new permission>**. Type in the new permission and check whether you want to allow or deny access from the remote address. To change a permission, select the remote address and click **Rename**. To remove a permission, select the remote address and click **Remove**. When you are finished, click **Save** to save your changes.

If the server is running, any new permissions will take effect as soon as you save the changes.

This window displays context-sensitive help. Move the cursor over a control or indicator for more information about it.

Figure 3.14- Measurement and Automation Explorer solving limited Access

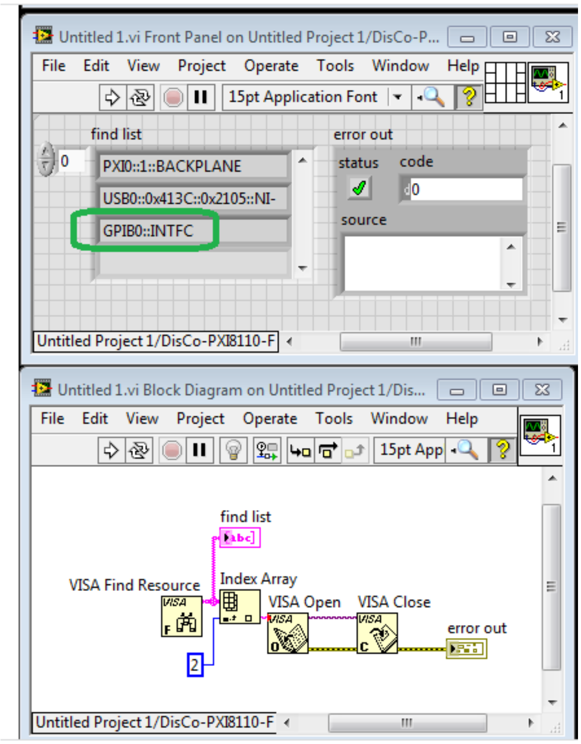
Error message occurrence when visa applications are being processed online -1043707192 in the device of the visa service in Veri Stand.


Untitled Project 1 * - Project Explorer
File Edit View Project Operate Tools Window Help
Items
Files

Project: Untitled Project 1
My Computer
Dependencies
Build Specifications
DisCo-PXI8110-F (10.1.128.193)
Untitled 1.vi
Dependencies
Build Specifications

Figure 3.15 - project explorer navigating Visa IP Address

Select Project and Right click on the dropdown options then choose untitled 1.vi


Untitled 1.vi Front Panel on Untitled Project 1/DisCo-P...
File Edit View Project Operate Tools Window Help
15pt Application Font
Untitled 1.vi Block Diagram on Untitled Project 1/Dis...
File Edit View Project Operate Tools Window Help
15pt App
find list
VISA Find Resource
Index Array
VISA Open
VISA Close
error out
2
Untitled Project 1/DisCo-PXI8110-F

find list
0
PXI0::1::BACKPLANE
USB0::0x413C::0x2105::NI-
GPIB0::INTFC

error out
status ✓
code 0
source

Untitled Project 1/DisCo-PXI8110-F

Figure 3.16 - block diagram on untitled project navigating Visa

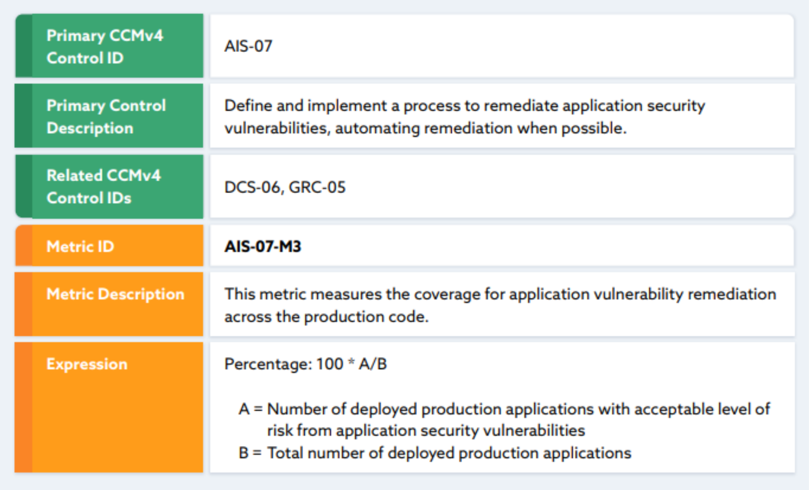
As shown in the diagrams above, one can take the address circled in green rather than that of visa and with this method, the message shown as error will vanish.

3.8 Implementations guidelines of metrics at visa Service

There must be a software inventory of deployed production code. The production code must be quantified based on the organization's definition of deployed code running in production. The same number should be used to measure AIS-07. The definition of deployed production code used for the software inventory should be aligned with security scanning, testing, and/or reporting methods where possible to simplify measurement. As the number of different deployment systems increase the likelihood of standardized deployment can decrease. The metric may be more suitable for an organization if the software deployment pipeline has multiple stages where change can be introduced and end-to-end validation cannot be done.

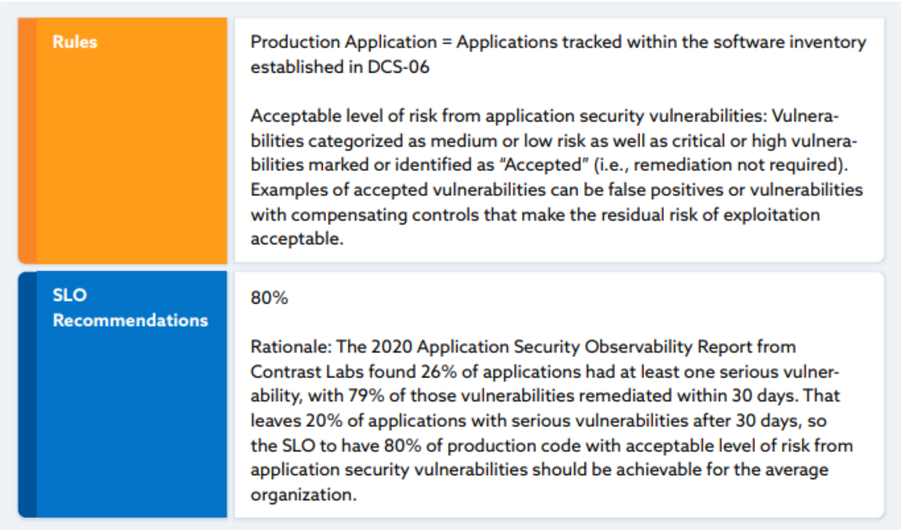
0%<=Percentage of steps in the software deployment pipeline that have an associated verification step<=100%

If deviations from the standard are approved, the system should account for and manage the exception as approved. This metric should be aligned with an organization's development or release cycle to provide timely input for correction in the next deployment or release. For Instance, if an organization uses an agile development methodology with two-week sprints, the metric should be measured at least every two weeks to provide data for review.



Primary CCMv4 Control ID	AIS-07
Primary Control Description	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.
Related CCMv4 Control IDs	DCS-06, GRC-05
Metric ID	**AIS-07-M3**
Metric Description	This metric measures the coverage for application vulnerability remediation across the production code.
Expression	Percentage: 100 * A/B A = Number of deployed production applications with acceptable level of risk from application security vulnerabilities B = Total number of deployed production applications

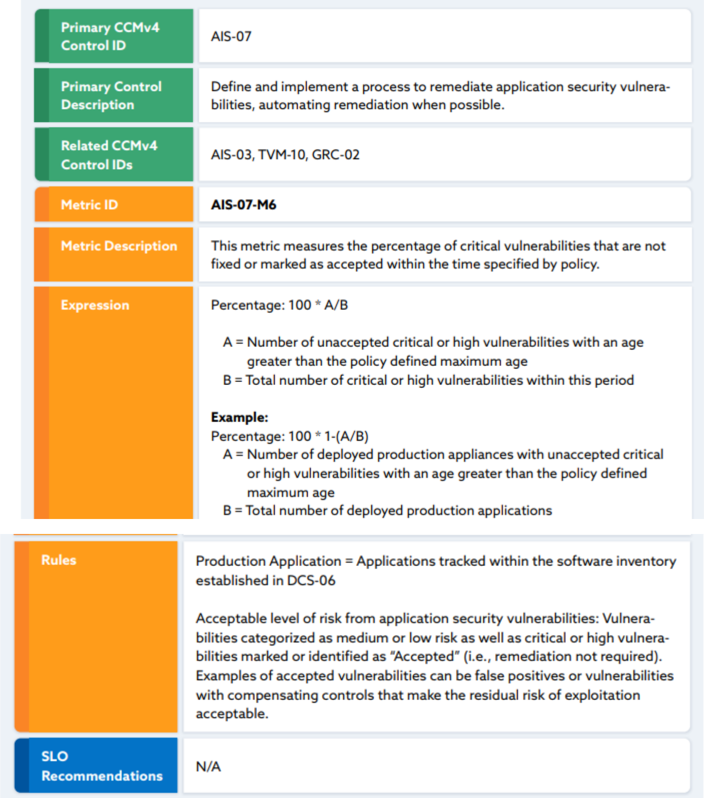
Figure 3.19a - CCC-03-M1



Rules	Production Application = Applications tracked within the software inventory established in DCS-06 Acceptable level of risk from application security vulnerabilities: Vulnerabilities categorized as medium or low risk as well as critical or high vulnerabilities marked or identified as "Accepted" (i.e., remediation not required). Examples of accepted vulnerabilities can be false positives or vulnerabilities with compensating controls that make the residual risk of exploitation acceptable.
SLO Recommendations	80% Rationale: The 2020 Application Security Observability Report from Contrast Labs found 26% of applications had at least one serious vulnerability, with 79% of those vulnerabilities remediated within 30 days. That leaves 20% of applications with serious vulnerabilities after 30 days, so the SLO to have 80% of production code with acceptable level of risk from application security vulnerabilities should be achievable for the average organization.

Figure 3.17 - Metric AIS-07-M3

The organization's vulnerability management guidelines should be used to define the acceptable level of risk. The common scoring system should be used to define the classification of vulnerabilities as critical risk. A vulnerability with a score of nine or higher is critical and a vulnerability with a score of seven or less is high risk.



Primary CCMv4 Control ID	AIS-07
Primary Control Description	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.
Related CCMv4 Control IDs	AIS-03, TVM-10, GRC-02
Metric ID	**AIS-07-M6**
Metric Description	This metric measures the percentage of critical vulnerabilities that are not fixed or marked as accepted within the time specified by policy.
Expression	Percentage: 100 * A/B A = Number of unaccepted critical or high vulnerabilities with an age greater than the policy defined maximum age B = Total number of critical or high vulnerabilities within this period **Example:** Percentage: 100 * 1-(A/B) A = Number of deployed production appliances with unaccepted critical or high vulnerabilities with an age greater than the policy defined maximum age B = Total number of deployed production applications
Rules	Production Application = Applications tracked within the software inventory established in DCS-06 Acceptable level of risk from application security vulnerabilities: Vulnerabilities categorized as medium or low risk as well as critical or high vulnerabilities marked or identified as "Accepted" (i.e., remediation not required). Examples of accepted vulnerabilities can be false positives or vulnerabilities with compensating controls that make the residual risk of exploitation acceptable.
SLO Recommendations	N/A

Figure 3.18 - Metric AIS-07

1. In the vulnerability management tool, it should be based on common vulnerability scoring system (CVSS).

2. Date and time of vulnerability discovery could be obtained from the vulnerability management tool as it scans and detects vulnerabilities.

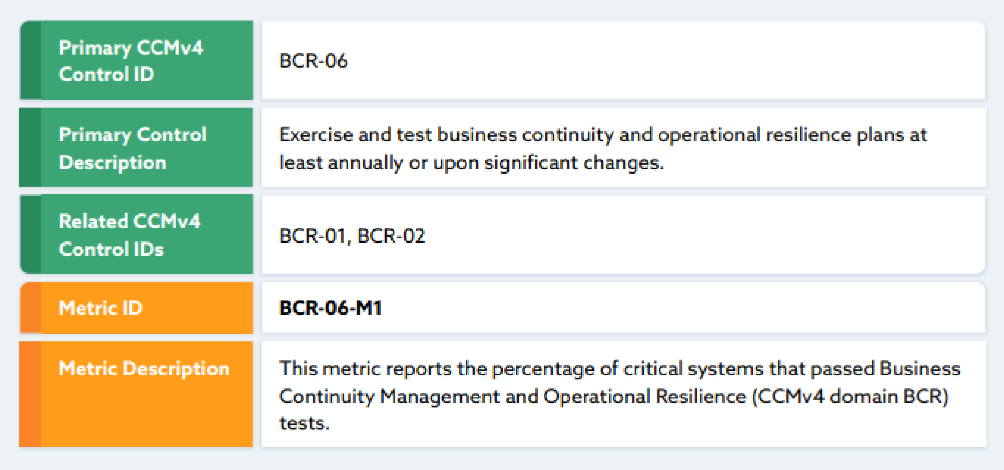
3. Date and time of vulnerability remediation or acceptance could be obtained in the following ways:

a. From the vulnerability management tool as it scans and finds that a previously detected vulnerability is not present nor detected.

b. From the patch, deploy tool (e.g., SCCM) as it successfully deploys and installs a patch that fixes an identified vulnerability.

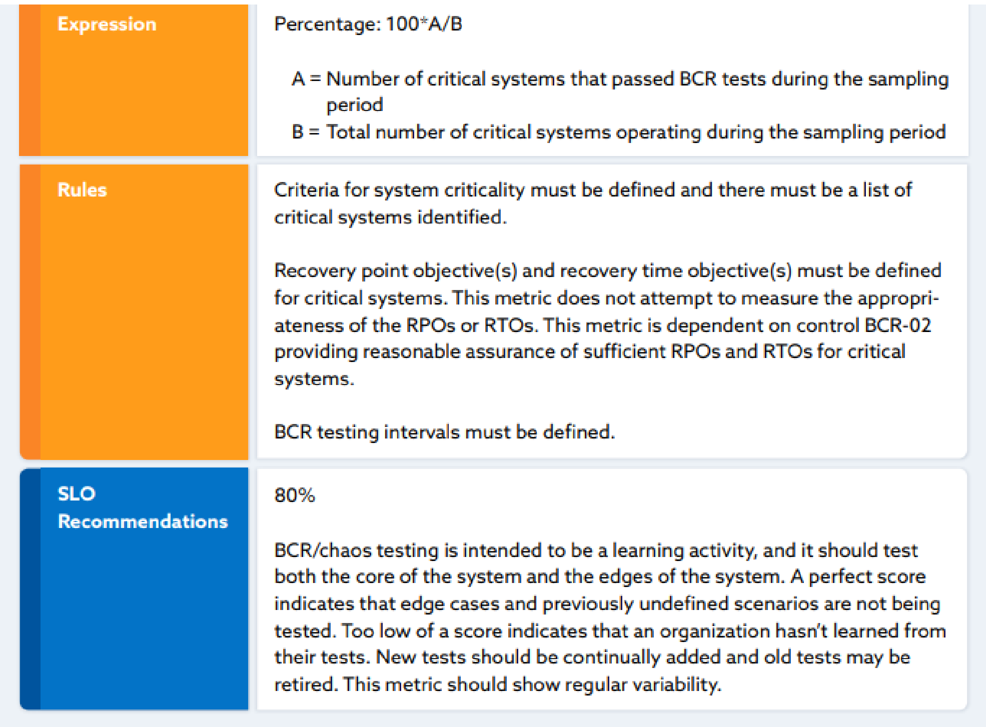
c. From the application/code release tool as it moves into production, the new version of the application does not contain the code vulnerability.

Frequent evaluation should be aligned with the frequency of vulnerability scans. (Scans should happen at least monthly but more often) recommended. Vulnerability scans can be done at a predefined frequency or when new code is built or deployed.



Primary CCMv4 Control ID	BCR-06
Primary Control Description	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.
Related CCMv4 Control IDs	BCR-01, BCR-02
Metric ID	**BCR-06-M1**
Metric Description	This metric reports the percentage of critical systems that passed Business Continuity Management and Operational Resilience (CCMv4 domain BCR) tests.

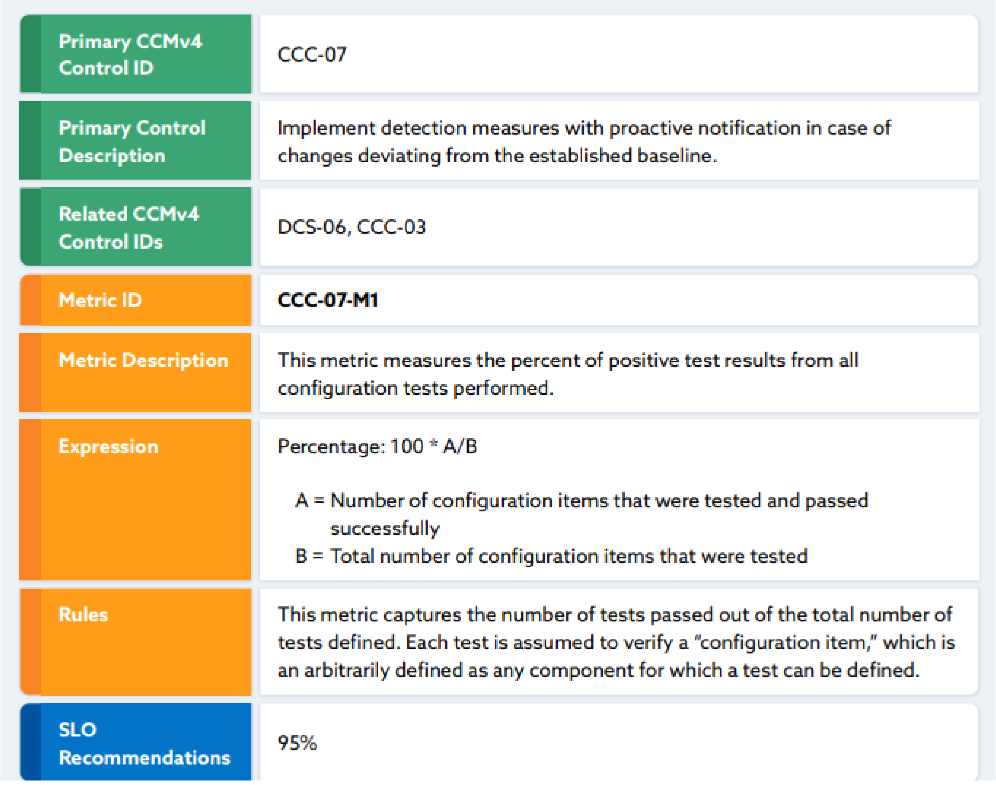
Figure 3.18a - Metric AIS-07



Expression	Percentage: 100*A/B A = Number of critical systems that passed BCR tests during the sampling period B = Total number of critical systems operating during the sampling period
Rules	Criteria for system criticality must be defined and there must be a list of critical systems identified. Recovery point objective(s) and recovery time objective(s) must be defined for critical systems. This metric does not attempt to measure the appropriateness of the RPOs or RTOs. This metric is dependent on control BCR-02 providing reasonable assurance of sufficient RPOs and RTOs for critical systems. BCR testing intervals must be defined.
SLO Recommendations	80% BCR/chaos testing is intended to be a learning activity, and it should test both the core of the system and the edges of the system. A perfect score indicates that edge cases and previously undefined scenarios are not being tested. Too low of a score indicates that an organization hasn't learned from their tests. New tests should be continually added and old tests may be retired. This metric should show regular variability.

Figure 3.19 - CCC-03-M1

The implementation guidelines for BCR-02 state that critical systems should be identified. According to the implementation guidelines for BCR-02, “Accessed” means achieving the RPO within the RTO defined for each critical system I the scope of the assessment/audit. The sampling period for this metric should align with the test intervals defined by the business continuity plan, in accordance with the CCMv4 implementation guidelines for BCR-04. BCR tests should include chaos test when possible production in. Chaos engineering is the discipline of experimenting on a software system in order to build confidence in the system’s capability to withstand turbulent and unexpected conditions.



Primary CCMv4 Control ID	CCC-07
Primary Control Description	Implement detection measures with proactive notification in case of changes deviating from the established baseline.
Related CCMv4 Control IDs	DCS-06, CCC-03
Metric ID	**CCC-07-M1**
Metric Description	This metric measures the percent of positive test results from all configuration tests performed.
Expression	Percentage: 100 * A/B A = Number of configuration items that were tested and passed successfully B = Total number of configuration items that were tested
Rules	This metric captures the number of tests passed out of the total number of tests defined. Each test is assumed to verify a "configuration item," which is an arbitrarily defined as any component for which a test can be defined.
SLO Recommendations	95%

Figure 3.20 - Metric CCC-07-M1

This metric needs the implementation of CCMv4 DCS-06. Assets cataloguing and Tracking as well as the capability to determine which assets or asset groups are deployed by automation. Given the dynamic nature of cloud environments, the metric can provide more value if the variation in the release management system's coverage over the population of assets is reported over time. The percentage of assets that fall within an accepted number of deviations gives stakeholders assurance of whether change control is getting better or worse.

Large populations of more than 1,000 assets can use six standard deviations as an acceptable level of change per time. Smaller populations of assets will need to use fewer standard deviations as an acceptable level of change maybe even just one deviation.

CHAPTER 4
OCCUPATIONAL SAFETY AND HEALTH

4.1 Regulations of Health and Safety

The purpose of this chapter on health and safety regulations is to include technological, sanitary, and medical preventive measures aimed at ensuring the health and ability of individuals to deal with them in addition to settle on ways and means to provide a successful and supportive work environment. The Health and Safety Regulation aims to ensure and improve the safety and health of workers at work by establishing responsibilities, rights and reciprocal ties between employers, employees and their representatives including institutions of the State.

4.2 Occupational Safety Management for Remote Office of State Institutes

The Effective planning of occupational safety management is important because of the effectiveness of worker's safety depends thereon to possess active occupational safety management. We have to make a management, which will successively create structural subdivisions for establishing safety and healthy working conditions. The health and safety management team at this state institution is responsible to make the subdivisions (workshops, departments, services) by their heads and leading experts appointed by the top of the health and safety management department. This person will actively perform or coordinate the labor protection service at the state institution.

Some of the main principles of the implementation of occupational safety management are:

- a priority of human (employee's) health and life over the state institution performance;
- implementation of the accident prevention principle;
- joint discussion of labor safety issues and personal responsibility for decisions and their implications;
- the regularity of labor protection management;
- Publicity of control and managerial decisions.

4.3 Key Management System Components for the Offices of the State Institution.

Some Key Management System Components that will be used in the offices of state institution:

- Communication/Feedback loops
- Continual Improvement/Learning
- Accountability/Responsibility
- Leadership
- Participation
- Concept of Integration

4.4 Structure of Labour Protection Service

Labour Protection Service and structure of the remote office of state institutes.

At the office of state institutions, Labour Protection services will include the following expertise:

- Special engineers;
- Occupational hygiene experts;
- Labour protection lawyers.

Under the Labour Protection service of the state institutions, a laboratory will be set up to control harmful substances at the workplaces.

4.5 Size of Occupational Safety Service

Occupational safety and service size at state institutions. The occupational safety and service size will be determined according to the number of workers working in the different offices of the state institution. Occupational safety service will participate in the following activities:

- o Investigation accidents and occupational diseases;
- o Formation of OS fund of
- o and its budget allocation;
- o Development of OS instructions;

o The activity of workplaces certification commission.

Injury’s analysis of occupation safety for a state institution.

Some of the methods, which we will use, for studying occupational injuries at state institution are as To ensure that occupational safety service functions properly and correctly. We will have to calculate the amount of employee’s base on the following formula presented below. For employees' number n > 500 persons, LP service size, defined by the formula:

M_1=2+(E_av*C_h)/R (2.1)

M_1=2+(450*100)/1800

M_1=27

where Eav is the average number of employees;

R is an annual effective production resource of LP expert R= 1800 hours;

Ch is a coefficient accounting for occupational hazard:

C_h=1+(E_b+E_a)/E_av (2.2)

C_h=1+(350+100)/400

C_h=2.125

Eb is the number of employers dealing with harmful substance regardless of their concentration; Ea is the number of employees engaged in increased-risk works who are annually certified in LP.

4.6 Occupational Injuries Analysis

follow:

- statistical;
- topographical;
- monographic;
- economic;
- questionnaire-based;
- Experts.

The monographic method is a detailed survey of work conditions, equipment, facilities, technology, hygiene, and sanitary conditions. Topographical method involves marking the accident spots at the workshop layout plan. The economic method is often wont to study and analyze losses caused by occupational injuries. Questionnaire-based method - Involves the event of questionnaire forms for workers. Expert method is often supported by expert conclusions on work conditions and compliance of the technology, equipment, facilities, and tools with the demands of standards and ergonomic regulations to machines, equipment, control boards, etc.

4.7 The responsibility of officials for violation of occupational safety

Violation and responsibility of officials that violate the occupational safety legislation at the office of the state institution.

- Disciplinary responsibility is necessary in cases where guilt is violated rules and regulations for safety. The violation does not lead to serious consequences and could result in reprimand or release.
- Administrative responsibility is imposed on perpetrators' fines. The right to impose fines using the occupational safety legislation of the offices of the state institution.
- Criminal responsibility occurs when irregularities may cause or have caused accidents to people or any other consequences. Criminal liability can carry only guilty parties, which because of their official position or by special order obliged to provide safe and healthy working conditions.
- Material responsibility of guilty officials for violation of safety rules occurs when the result of severe violations at the state institution will be required During the accident, as well as during the elimination or removal of some office equipment at the facilities;
- During working hours when moving on foot or by public transport with an employee whose work is, connected with the movement of objects between services. to pay certain sums of money to the victim of an accident or the social insurance to compensate for these payments.

4.8 Investigation and registration of accidents and occupational diseases

Accidents, Investigations, Registration, and Occupational diseases may occur to any employee who works with the state institution. These are the types of accidents that occur, according to the result of the investigation: injuries, occupational diseases, and acute poisoning, heatstroke, frostbite, drowning, electric shock, and lightning damage due to accidents, fires, natural disasters, contact with animals and insects:

- While performing job duties (including an official trip), and actions in favor of the state institution even without the authorization of the institution;
- At the workplace, on the premises or at another workplace, given the set break;
- On the time required for remediation of the means of protection, clothes before and after work, as well as facilities for personal hygiene;
- While traveling to or from work in transport provided by the state institution, as well as personal vehicles used for the benefit of the institution with permission from the institution;
-

4.9 Prevention of occupational injuries at a state institution

In the field of injury prevention, a special place belongs to the training and instruction of employees on safe working methods. After a few years of practice, this system has established a consistent means of teaching safe methods of labor. The introductory briefing is that the first phase of coaching on safe working practices, it is compulsory for all who get employment at the state institution be it (workers, engineers, students during part-time). The introductory briefing is going to be, conducted by a security engineer or chief engineer at the institution. Typically, the instruction is for 1.5–2 hours, and if the individual work hour is for 5–4 hours.

Content of introductory briefing:

- The main statement of the legislation on health and safety.
- Internal labor regulations and behavior in the institution premises.

- The route through the territory, the location of buildings, meaning of warning signs, colors, security, sound, and light alarm.
- Brief descriptions of particularly hazardous work and prevention accident measures (moving equipment, gas-flame treatment of metal).
- Some specific circumstances and causes of cases have occurred as a result of violations of safety instructions and discipline.

This chapter discusses the administration of the workplace safety, labor health programs and the study of occupational injuries. All of the recent health and safety management topics listed remind us of the effectiveness of LAN production for remote offices of state institutions.

CONCLUSION

To conclude, the research paper covers the methods of increasing the security level of the information and communication system of visa service and other facilitated terms attributed to Aspirational smart travel and visa facilitation services. On this basis, here are a few points of the outlined policy challenges.

a. There are two obvious obstacles to a wide implementation of a national smart Travel system and financing the infrastructure and ensuring global operability. In fact, many countries are suffering from severe budgetary constraints and lack the resources for significant infrastructure investment. For a successful investment in Smart Travel technology to have the desired return, the system must be a combination of compatible technological regimes, which do not merely mimic the existing paper visa regime.

b. International leadership will be critical to ensure that efforts to modernize visa policies and travel security infrastructure are standardized but reflect different cultural preferences for the protection of data privacy. On a national level, countries will need to clarify responsibility and ensure cooperation between the various institutions involved in the process. Moreover, a number of policy reforms and new cooperation models will be needed with different government agencies and public-private partnerships.

c. However, countries must start by recognizing and responding to the economic benefits that can be generated by smarter travel. Much can be done on national and bilateral levels to abolish visa restrictions. As states pursue new trade and economic links with their economic partners, they should expand the discussions to include shared goals for travel policy.

d. From these discussions will come a reshaping of the travel environment to create an efficient, secure, globally compatible and minimally intrusive system for approving and screening the smart travelers of the future.

However, I would recommend that visa service take into consideration the following points when implementing metrics guidelines. The main benefit of developing metrics is that it allows the creation of a continuous auditing process, which allows an organization to show control compliance at all times. To understand why this is important it is useful to examine some of the shortcomings of traditional assurance mechanisms. Traditional security assurance is based on verifying those controls are correctly selected, designed, implemented, enforced, and monitored.

This process is largely a manual task done by humans through evidence and documentation review and repeated every 6 or 12 months. This approach has solidified over the years through standardization and best practices, but in today’s cloud-centric environment it suffers from many important shortcomings. Therefore, the following points is highly recommended in auditing and securing visa organizations.

First, if we want to get more continuous assurance regarding the security of the information system, this traditional approach does not scale in terms of cost and feasibility. Manual or semi-automated assessments processes designed to be conducted every six months are unlikely applicable for verifications that are expected to be performed daily or hourly.

Second, while traditional security assessments seem appropriate for policy and procedural controls, they are not appropriate for the evaluation of technical security measures. This is especially the case when they are applied to environments that are constantly changing while being exposed to changing threats and vulnerabilities. It makes sense to implement automated and continuous assessments of technical measures, as many organizations already do and we can even extend that idea to policy and procedural controls while evaluation of policy and procedural controls cannot be directly automated. We can implement automated techniques for the collection of evidence to prove their effectiveness.

Third, humans make mistakes when they do reviews repeatedly. In contrast, an automated assessment can be repeated indefinitely, without mistake, provided that the underlying tools are trustworthy. As a consequence of the shortcomings of traditional assurance tools, organizations who want continuous assurance must reconsider their approach to security assessments.

For continuous assurance, manual assessments must be traded for automated measurements, which largely leave humans out of the loop. Instead of assessing controls directly, tools are used to measure the security attributes of an information system and determine whether controls are put in place. For example, consider the Supply Chain Management, Transparency, and Accountability domain of CCMv4, which contains 14 control objectives. Taken together, the goal of these control objectives is to ensure that adequate tools, policies, and procedures are in place to establish, document, approve, communicate, apply, evaluate, and maintain the supply chain of CSP products and services.

REFERENCES

1. Visa Facilitation Service Sustainability Report. Retrieved 2020-2021 by Production Team. [Electronic Resource] Access Mode: Url: https://www.vfsglobal.com/en/PDF/CSR/sustainability-report-2020.pdf

2. Whitman M. Management of Information Security / Michael Whitman. Herbert Matford – Cengage Learning. 2013. -576p.

3. Visa Facilitation Service. Retrieved 15 October 2015. [Electronic Resource] Access Mode: Url:https://en.wikipedia.org/wiki/VFS_Global

4. World Economic Forum. Retrieved 1971. [Electronic Resource] Access Mode: Url:

   https://www3.weforum.org/docs/GAC/2014/WEF_GAC_TravelTourism_SmartTravel_WhitePaper_2014.pdf

5. Visa Facilitation Service Sound and Communication. Retrieved June 27, 2021. [Electronic Resource] Access Mode: Url: https://www.vfsfire.com/sound-communication/#tab-id-1

6. Serpent Visa management Software. Retrieved October 2020. [Electronic Resource] Access Mode: Url: https://www.serpentcs.com/serpentcs-visa-management-software-features-500#

7. Chennai Visa processing System Company. Retrieved 2019. [Electronic Resource] Access Mode: Url: https://www.excelanto.com/visa-processing-system-company-chennai.php

8. Knowledge Data Security Model Article. Retrieved 1960. [Electronic Resource] Access Mode: Url:

   https://knowledge.ni.com/KnowledgeArticleDetails?id=kA00Z0000019MAZSA2&l=ru-UA

9. National Institute of Standards and Technology. Retrieved 2020, June 22. Pg 522-533. Computer Security Resource Center: Automated Cryptographic Validation Testing. NIST. Access Mode: [Electronic Resource] URl: https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing

10. Open Metrics. (n.d.). The OpenMetrics project creating a standard for exposing metrics data. Retrieved October 7, 2021. Access mode: [Electronic Resource] URL: https://openmetrics.io/

11. Apache Spark 3.2.0 Documentation: Access Mode: [Electronic Resource] Url: https://spark.apache.org/docs/latest/

12. Open Web Application Security Project. Access Mode: [Electronic Resource] URL: https//owasp.org/.

APPENDIX A TITLE PAGE

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

МАТЕРІАЛИ

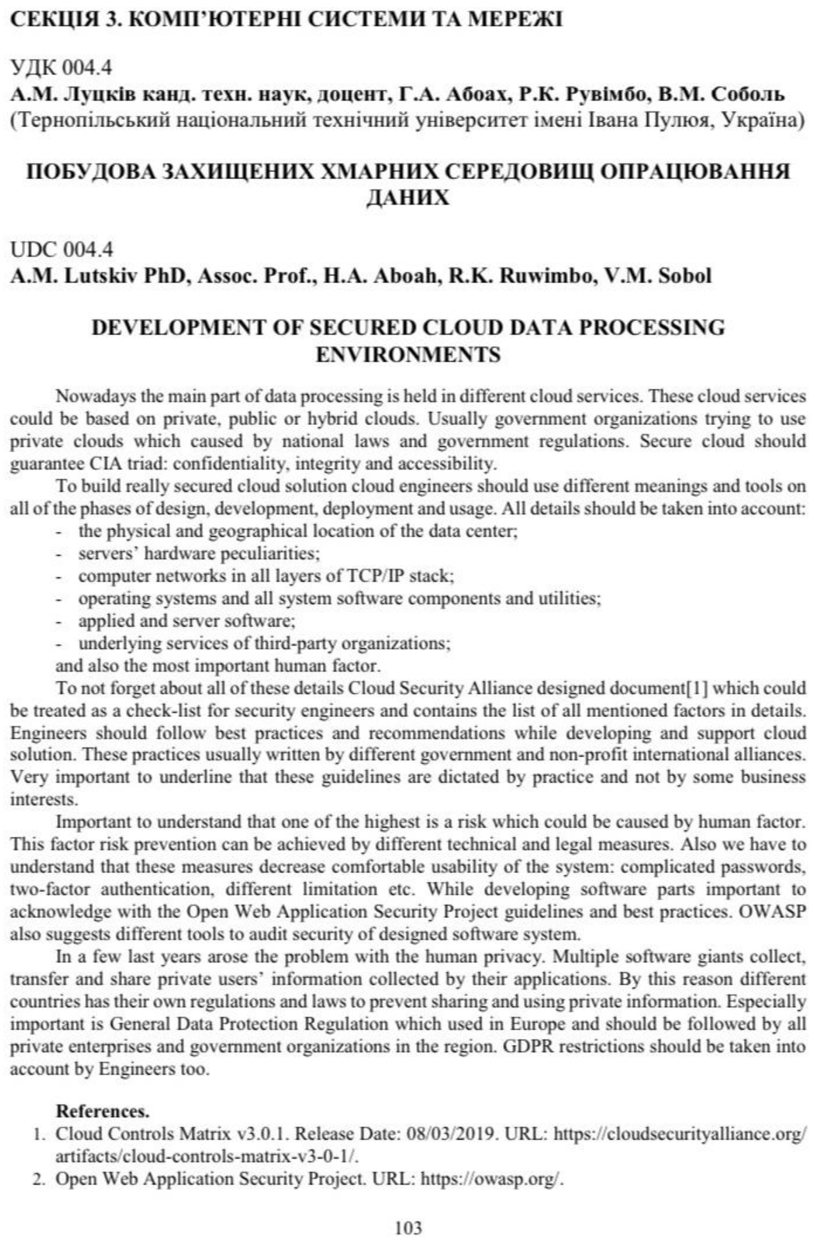
IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

APPENDIX B



СЕКЦІЯ 3. КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

УДК 004.4

А.М. Луцків канд. техн. наук, доцент, Г.А. Абоах, Р.К. Рувімбо, В.М. Соболь
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОБУДОВА ЗАХИЩЕНИХ ХМАРНИХ СЕРЕДОВИЩ ОПРАЦЮВАННЯ ДАНИХ

UDC 004.4

A.M. Lutskiv PhD, Assoc. Prof., H.A. Aboah, R.K. Ruwimbo, V.M. Sobol

DEVELOPMENT OF SECURED CLOUD DATA PROCESSING ENVIRONMENTS

Nowadays the main part of data processing is held in different cloud services. These cloud services could be based on private, public or hybrid clouds. Usually government organizations trying to use private clouds which caused by national laws and government regulations. Secure cloud should guarantee CIA triad: confidentiality, integrity and accessibility.

To build really secured cloud solution cloud engineers should use different meanings and tools on all of the phases of design, development, deployment and usage. All details should be taken into account:

- the physical and geographical location of the data center;
- servers' hardware peculiarities;
- computer networks in all layers of TCP/IP stack;
- operating systems and all system software components and utilities;
- applied and server software;
- underlying services of third-party organizations;

and also the most important human factor.

To not forget about all of these details Cloud Security Alliance designed document[1] which could be treated as a check-list for security engineers and contains the list of all mentioned factors in details. Engineers should follow best practices and recommendations while developing and support cloud solution. These practices usually written by different government and non-profit international alliances. Very important to underline that these guidelines are dictated by practice and not by some business interests.

Important to understand that one of the highest is a risk which could be caused by human factor. This factor risk prevention can be achieved by different technical and legal measures. Also we have to understand that these measures decrease comfortable usability of the system: complicated passwords, two-factor authentication, different limitation etc. While developing software parts important to acknowledge with the Open Web Application Security Project guidelines and best practices. OWASP also suggests different tools to audit security of designed software system.

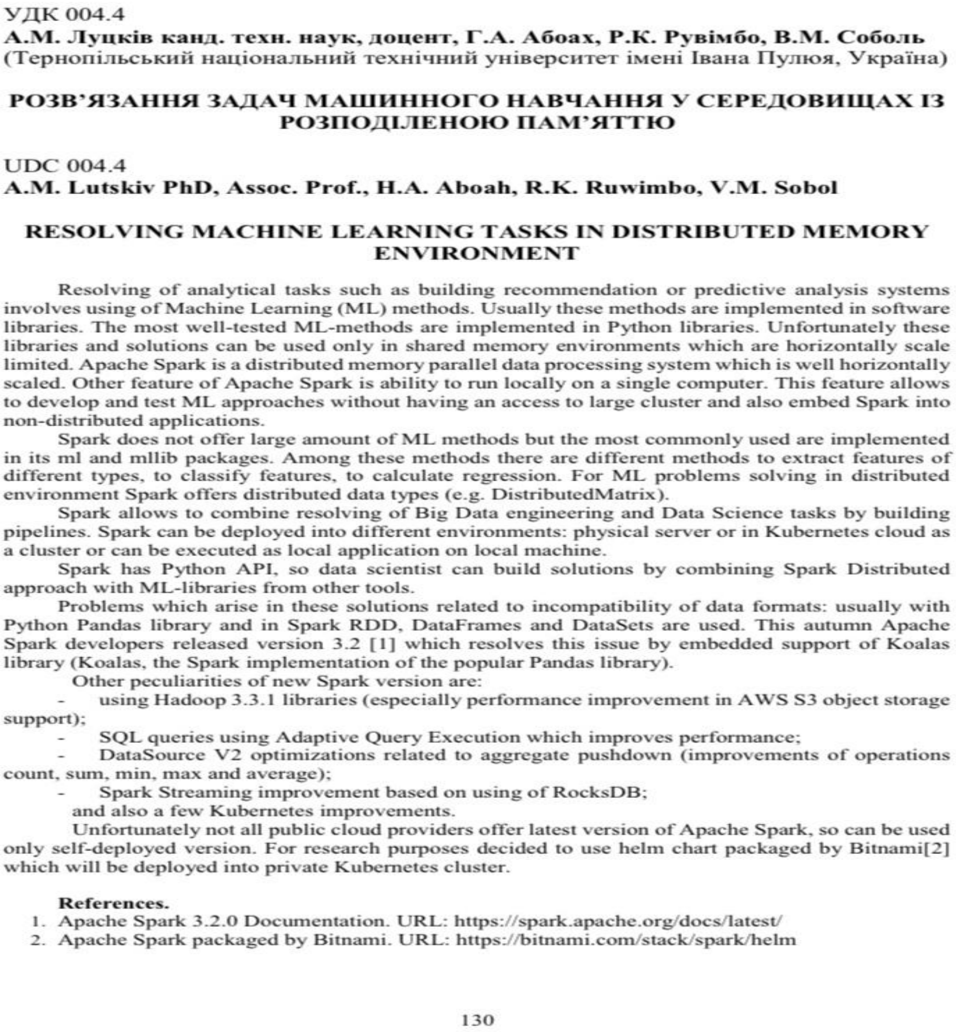
In a few last years arose the problem with the human privacy. Multiple software giants collect, transfer and share private users' information collected by their applications. By this reason different countries has their own regulations and laws to prevent sharing and using private information. Especially important is General Data Protection Regulation which used in Europe and should be followed by all private enterprises and government organizations in the region. GDPR restrictions should be taken into account by Engineers too.

References.

1. Cloud Controls Matrix v3.0.1. Release Date: 08/03/2019. URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/.
2. Open Web Application Security Project. URL: https://owasp.org/.

Appendix B – precept from Technical Conference 2021

APPENDIX C



УДК 004.4

А.М. Луцків канд. техн. наук, доцент, Г.А. Абоах, Р.К. Рувімбо, В.М. Соболь
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗВ'ЯЗАННЯ ЗАДАЧ МАШИННОГО НАВЧАННЯ У СЕРЕДОВИЩАХ ІЗ РОЗПОДІЛЕНОЮ ПАМ'ЯТТЮ

UDC 004.4

A.M. Lutskiv PhD, Assoc. Prof., H.A. Aboah, R.K. Ruwimbo, V.M. Sobol

RESOLVING MACHINE LEARNING TASKS IN DISTRIBUTED MEMORY ENVIRONMENT

Resolving of analytical tasks such as building recommendation or predictive analysis systems involves using of Machine Learning (ML) methods. Usually these methods are implemented in software libraries. The most well-tested ML-methods are implemented in Python libraries. Unfortunately these libraries and solutions can be used only in shared memory environments which are horizontally scale limited. Apache Spark is a distributed memory parallel data processing system which is well horizontally scaled. Other feature of Apache Spark is ability to run locally on a single computer. This feature allows to develop and test ML approaches without having an access to large cluster and also embed Spark into non-distributed applications.

Spark does not offer large amount of ML methods but the most commonly used are implemented in its ml and mllib packages. Among these methods there are different methods to extract features of different types, to classify features, to calculate regression. For ML problems solving in distributed environment Spark offers distributed data types (e.g. DistributedMatrix).

Spark allows to combine resolving of Big Data engineering and Data Science tasks by building pipelines. Spark can be deployed into different environments: physical server or in Kubernetes cloud as a cluster or can be executed as local application on local machine.

Spark has Python API, so data scientist can build solutions by combining Spark Distributed approach with ML-libraries from other tools.

Problems which arise in these solutions related to incompatibility of data formats: usually with Python Pandas library and in Spark RDD, DataFrames and DataSets are used. This autumn Apache Spark developers released version 3.2 [1] which resolves this issue by embedded support of Koalas library (Koalas, the Spark implementation of the popular Pandas library).

Other peculiarities of new Spark version are:

- using Hadoop 3.3.1 libraries (especially performance improvement in AWS S3 object storage support);
- SQL queries using Adaptive Query Execution which improves performance;
- DataSource V2 optimizations related to aggregate pushdown (improvements of operations count, sum, min, max and average);
- Spark Streaming improvement based on using of RocksDB;

and also a few Kubernetes improvements.

Unfortunately not all public cloud providers offer latest version of Apache Spark, so can be used only self-deployed version. For research purposes decided to use helm chart packaged by Bitnami[2] which will be deployed into private Kubernetes cluster.

References.

1. Apache Spark 3.2.0 Documentation. URL: https://spark.apache.org/docs/latest/
2. Apache Spark packaged by Bitnami. URL: https://bitnami.com/stack/spark/helm

Appendix C – precept from Technical Conference 2021