CLOUD AS A CERTIFICATE

WHAT IS INTERESTING IN THE CCSP CERTIFICATION?

INTRODUCTION

- György Kollár
  - Electrical Engineer, (Old School Informatics)
  - Small Business Owner
  - Technical Director since 1991
  - Early Adopter type
  - Working in Security in the last 13 years
  - CISSP (2005-), CCSP (2016-)
  - Collecting old HP calculators

ABOUT THE CLOUD

- Everybody uses it

- It costs nothing

- Soneone takes care of everything

- It will always be there

- IT IS SAFE!

ABOUT CCSP

- Joint certification of (ISC)^2 and CSA (Cloud Security Alliance)

- „A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration."

- Successful candidates are competent in the following 6 domains

SIX DOMAINS OF COMMON BODY OF KNOWLEDGE (CBK)

1. Architectural Concepts and Design Requirements
2. Cloud Data Security
3. Cloud Platform and Infrastructure Security
4. Cloud Application Security
5. Operations
6. Legal and Compliance

EXPERIENCE REQUIREMENTS

- Minimum of 5 years experience

- Or

- CISSP credential

EXAMINATION

Length of exam	4 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

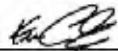## International Information System Security Certification Consortium

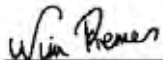The (ISC)² Board of Directors hereby awards

Gyorgy Kollar

the credential of

Certified Cloud Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Dr. Kevin Charest - Chairperson

Wim Remes - Secretary

CCSP®

84665
Certification Number

4/30/2019
Expiration Date

Certified Since: 2016

(ISC)²

DOMAIN 1:
ARCHITECTURAL CONCEPTS AND DESIGN REQUIREMENTS

- Cloud Computing Concepts

- Cloud Reference Architecture

- Security Concepts Relevant to Cloud Computing

- Design Principles of Secure Cloud Computing

- Trusted Cloud Services
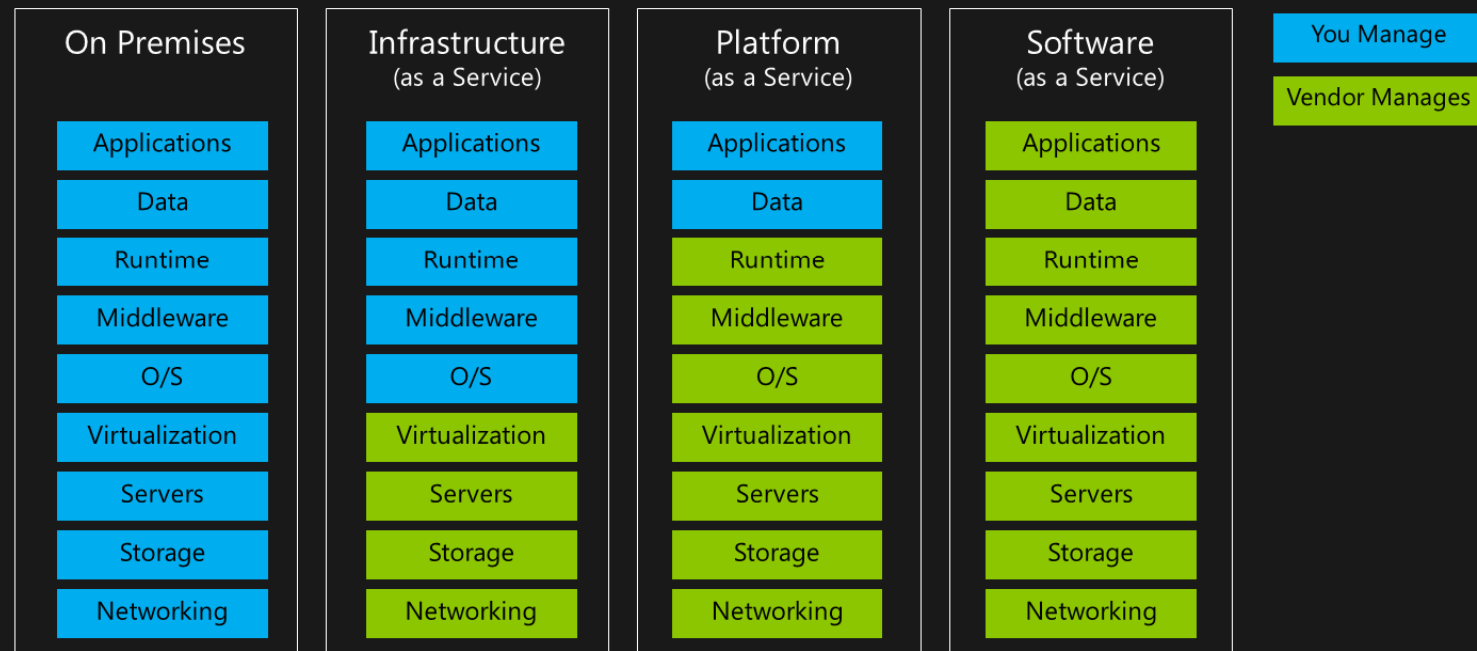
MEANING OF CLOUD

- on-demand self-service,

- broad network access,

- resource pooling,

- rapid elasticity or expansion,

- measured service

"SERVICE MODELS"

- Software,
- Platform,
- Infrastructure

Cloud Services

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

You Manage

Vendor Manages

"DEPLOYMENT MODELS"

- Private,

- Public,

- Community,

- Hybrid

DOMAIN 2:
CLOUD DATA SECURITY

- Cloud Data Lifecycle

- Cloud Data Storage Architectures

- Data Security Strategies

- Data Discovery and Classification

- Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PII)

- Data Rights Management

- Data Retention, Deletion, and Archiving Policies

- Auditability, Traceability and Accountability of Data Events

MOVING TO THE CLOUD

- CRM
  - Customer database
  - Scheduler
  - Financial data
- Project management
  - Subcontractors
  - Time management
  - Calculations
- Design documents
  - Schematics
  - Mechanical drawings
  - Software
  - Network diagrams
- Bookkeeping
  - Tax forms
  - Invoices

CHANGES IN THE CLOUD

- Where is my data?

- Where is my backup?

- How can I use my systems?

- How can I secure my systems?

- How can I delete my data?
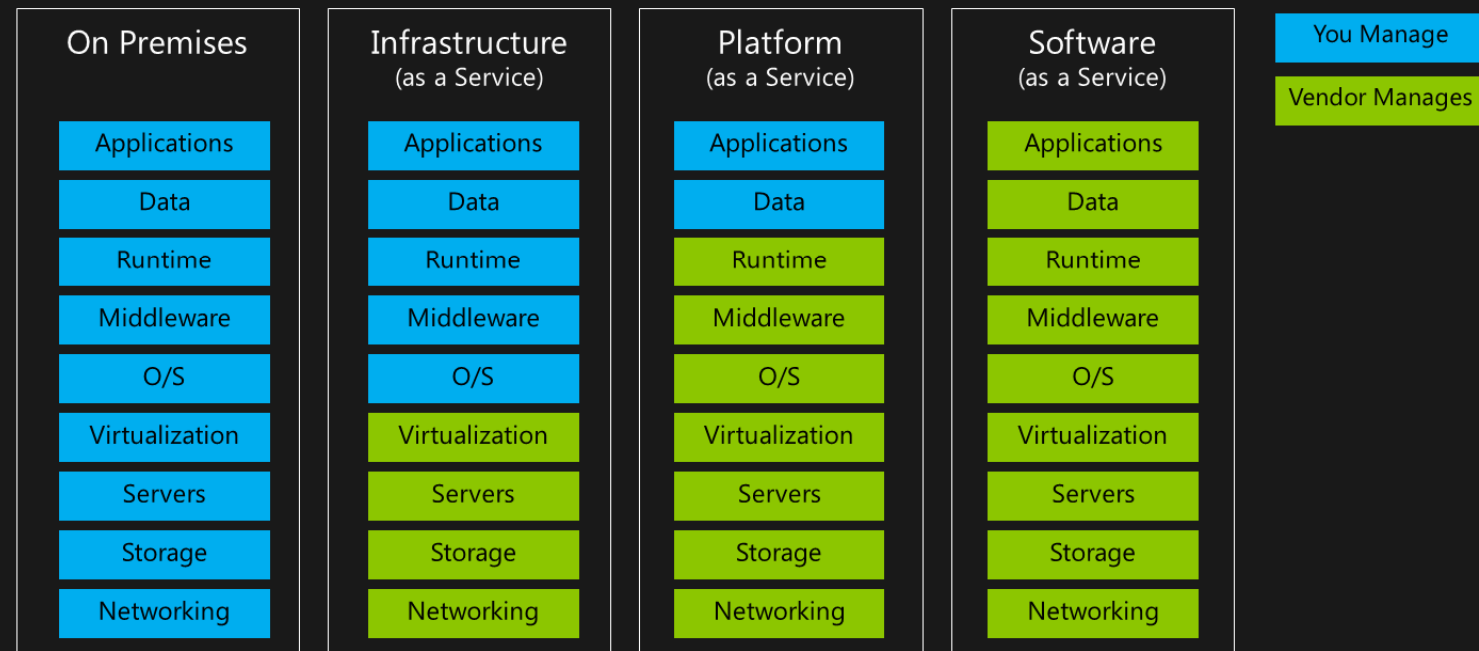
RISKS SHIFTED AND CHANGED

- Assets
  - Who owns the asset?
  - Who is responsible for the asset?
  - What asset?

"SERVICE MODELS"

- Software,
- Platform,
- Infrastructure

Cloud Services

On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

You Manage

Vendor Manages

DOMAIN 3:
CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

- Cloud Infrastructure Components

- Risks Associated to Cloud Infrastructure

- Design and Plan Security Controls

- Plan Disaster Recovery and Business Continuity Management

LAYERED SECURITY

- Phisical Layer
  - Cabling
  - Services
  - Power
  - HVAC
  - Emergency

DOMAIN 4:
CLOUD APPLICATION SECURITY

- Training and Awareness

- Cloud Software Assurance and Validation

- Use Verified Secure Software

- Software Development Life-Cycle (SDLC) Process

- Apply the Secure Software Development Life-Cycle the Specifics of Cloud Application Architecture

- Identity and Access Management

DOMAIN 5: OPERATIONS

- Support the Planning Process for the Data Center Design
- Implement and Build/ Run / Manage Physical Infrastructure for Cloud Environment
- Build/ Run / Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls
- Conduct Risk Assesment to Logical and Physical Infrastructure
- Understand the Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

DIFFERENCES BETWEEN CLASSIC AND CLOUD ENVIRONMENTS

- Size matters
  - Redundancy needs at least two of everything
- Cost matters
  - If you can share resources you can share costs
- Location matters
  - You want to reach it from anywhere, don't you?

On-Premise vs. Cloud

DOMAIN 6:
LEGAL AND COMPLIANCE

- Legal Requirements and Unique Risks within the Cloud Environment

- Privacy Issues, Including Jurisdictional Variation

- Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

- Implications of Cloud to Enterprise Risk Management

- Outsourcing and Cloud Contract Design

- Vendor Management

GDPR AND OTHER REGULATIONS

- Location

- Local Law

- Customer Country Law

- Etc.

RESPONSIBILITIES

- You can outsoure everything but responsibility

- But…
  - You can buy services
  - Make contracts
  - Share risks

- If you want something to be done put it into the contract

COSTS AND BENEFITS

- Efficiency

- Reliability

- Security

- Vendor lock-in

- Service drift

MOST OVERLOOKED THINGS

- Backup (and restore!)

- Upgrades

- Patch management

- Vulnerability management

- Confidentiality

- Privacy

CLOUD GUIDE

- Security is not something for free

- It will not be included if you do not ask for it

- Checking everything is a must

- Read the small text as well

- Encryption is necessary

- Keep a clear way out

CONCLUSION

- Cloud is the next big thing

- This knowledge is on high demand

- There are lots of opportunities

- Cloud security is extremly inextricable (impossible to disentangle or separate.)

- References: www.isc2.org/ccsp-cbk-references