Information Security in the Cloud

Confidentiality - Integrity - Availability

Erik Marcussen

Deputy CTO
Unit4

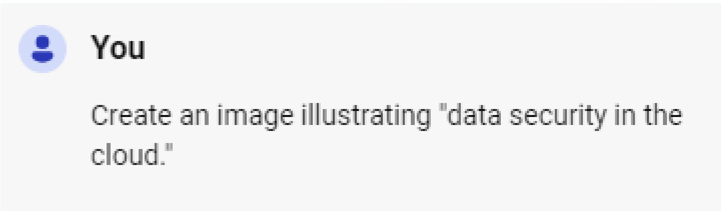
Welcome

Join our webinar for an in-depth look at how Unit4 can support your efforts to safeguard data, the core principles of information security and how they apply to modern technology.

High level topics for today:

- Shared Responsibility of Information Security in the Cloud
- Ensuring Confidentiality, Integrity, and Availability in Unit4's Cloud Services
- Building a Strong, Security-Focused Organization
- AI: Enhancing Protection and Introducing New Threats

Warning: this presentation includes AI-generated content!



You

Create an image illustrating "data security in the cloud."

CIA – a framework for information security

Confidentiality

Securing information is not available for unauthorized people

Integrity

Securing information is not modified unintentionally, or by unauthorized people

Availability

Securing information is available for authorized people when needed

Robustness: The organization and the systems are resilient, and able to restore business as usual after incidents

The cloud shared security model

🟩

Customer responsibility

Data classification and data ownership

🟩/⬛

Shared responsibility

Identity, access management, configuration

⬛

SaaS provider responsibility

Physical | Infrastructure | Service | Application

Responsibility	On-Prem	SaaS
Data classification and accountability	🟩	🟩
Client- and endpoint protection	🟩	🟩
Identity and access management	🟩	🟩/⬛
Application- and service level controls	🟩	🟩/⬛
Network controls	🟩	⬛/🟦
Infrastructure	🟩	⬛/🟦
Physical security	🟩	🟦

🟩 Customer ⬛ SaaS provider / Unit4 🟦 Cloud platform provider / Microsoft Azure

01 Confidentiality

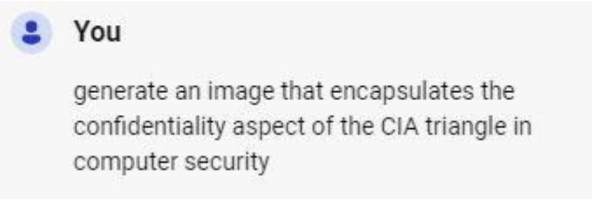
How is confidentialty ensured?

- Secure authentication
- Proper access control / configuration

- Application security
- Service security
- Infrastructure security
- Client security

- Encryption ”at rest”
- Encryption ”in transit”
- Privacy by design

- Monitoring



You

generate an image that encapsulates the confidentiality aspect of the CIA triangle in computer security

Zero Trust Guiding Principles

Continuously verify

Authenticate and authorize based on all available data points.

Least privilege access

Limit access to just enough access, just when needed (JIT/JEA)

Assume breach

Minimize consequences and segment access

Without compromises for the employee’s productivity

02 Integrity

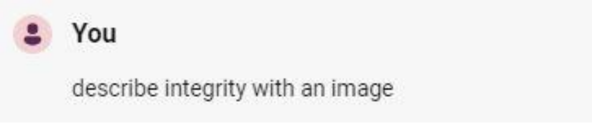
How is integrity ensured?

- Unquestionable data ownership
- Approval routines
- Correct configuration and automation

- Data validation upon entry
- Data source and quality control
- Client security / Zero Trust

- Message signing
- End-to-end encryption

- Audit logs
- Access logs



You

describe integrity with an image

03 Availability

Availability – Service Level Agreement

99.8 %

Availability

< 1t RPO

< 12t RTO

Lowest average availability

«Recovery Point Objective»

Maximum data loss in the event of a serious incident

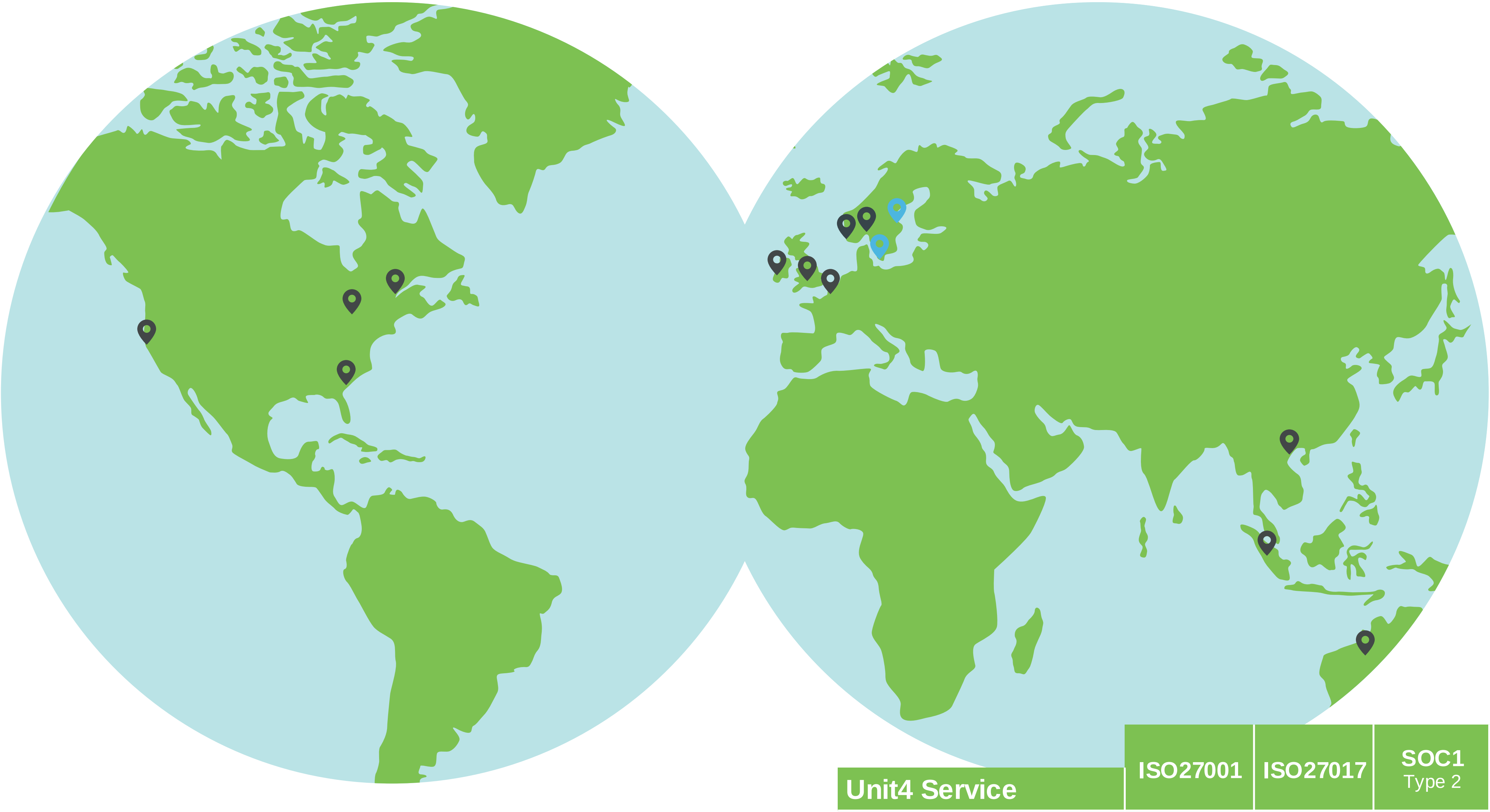
(Robustness)

«Recovery Time Objective»

Maximum time before the data is restored in the event of a serious incident

(Robustness)

Unit4 Cloud



Unit4 Service	ISO27001	ISO27017	SOC1 Type 2	SOC2 Type 2
Unit4 SaaS - **Cloud**	✓	✓	✓	✓

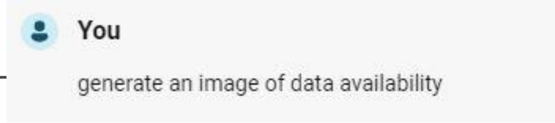
How is availability ensured?

- ”Sea of green” - SLA
- Quick response / automation
- Phased roll-out of changes
- Avoid any manual infra configuration

- End point control
- Intelligent blocking and rerouting
- Redundancy

- Continuous backup
- Rapid re-establishment of complete systems

- Health monitoring everywhere
- Monitoring / SIEM
- Automatic notifications



You

generate an image of data availability

04 Unit4 and AI

Unit4's smart automation solutions

Human-centric approach

- Understanding user needs
- Integration into the experience
- Technology selection and implementation

Pragmatic AI

- Development is driven by user problems
- AI on when traditional methods fall short

Ethical Responsibility

- Ensuring responsible progress
- User data protection

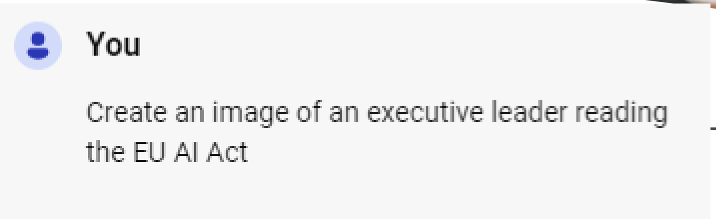
Security and AI

EU AI Act

- Ban on systems with unacceptable risk
- Obligations for suppliers and users of high-risk systems
- Requirements for the development of general AI-systems, including ethical considerations
- Openness around training data and method
- Transparency about precision and required ability to override

New considerations for the development and use of AI

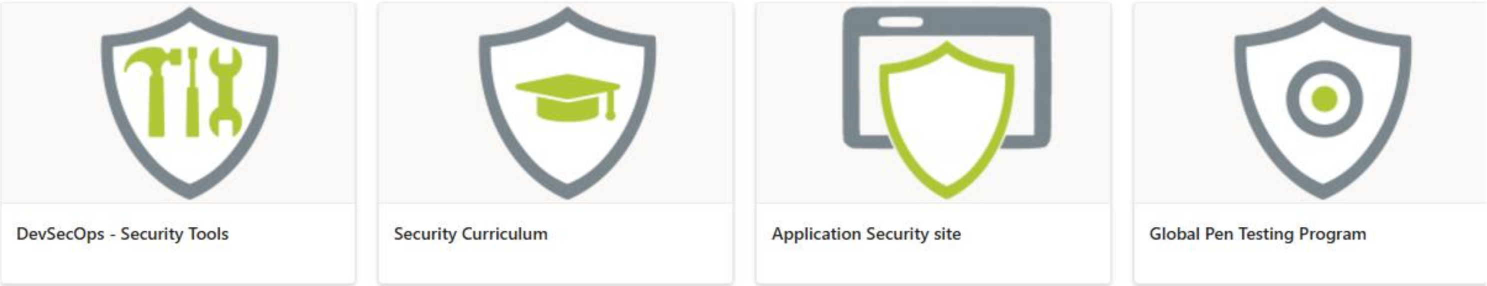
- Neutrality, bias, ethics, and copyright
- Intuitive visibility of when AI is involved in a decision
- Awareness among users on possibilities and limitations
- Careful use of data in both training and operational phases
- Introduces completely new attack vectors



Create an image of an executive leader reading the EU AI Act

05 Robustness

Security as part of Unit4's Software Development Lifecycle



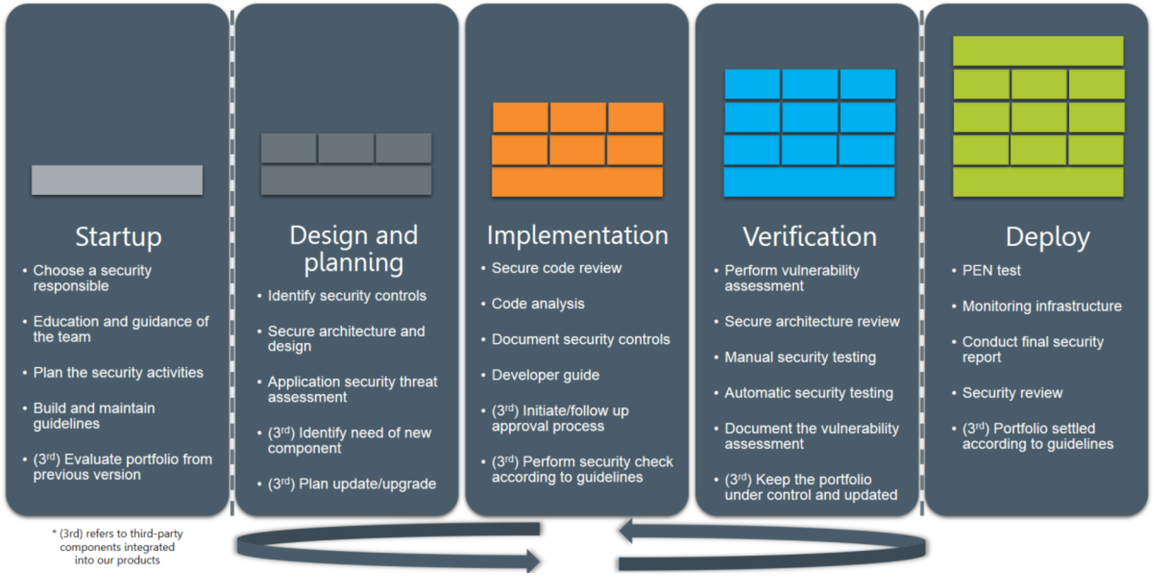
DevSecOps - Security Tools

Security Curriculum

Application Security site

Global Pen Testing Program

Global Quality Assurance Standard



Startup

- Choose a security responsible
- Education and guidance of the team
- Plan the security activities
- Build and maintain guidelines
- (3rd) Evaluate portfolio from previous version

Design and planning

- Identify security controls
- Secure architecture and design
- Application security threat assessment
- (3rd) Identify need of new component
- (3rd) Plan update/upgrade

Implementation

- Secure code review
- Code analysis
- Document security controls
- Developer guide
- (3rd) Initiate/follow up approval process
- (3rd) Perform security check according to guidelines

Verification

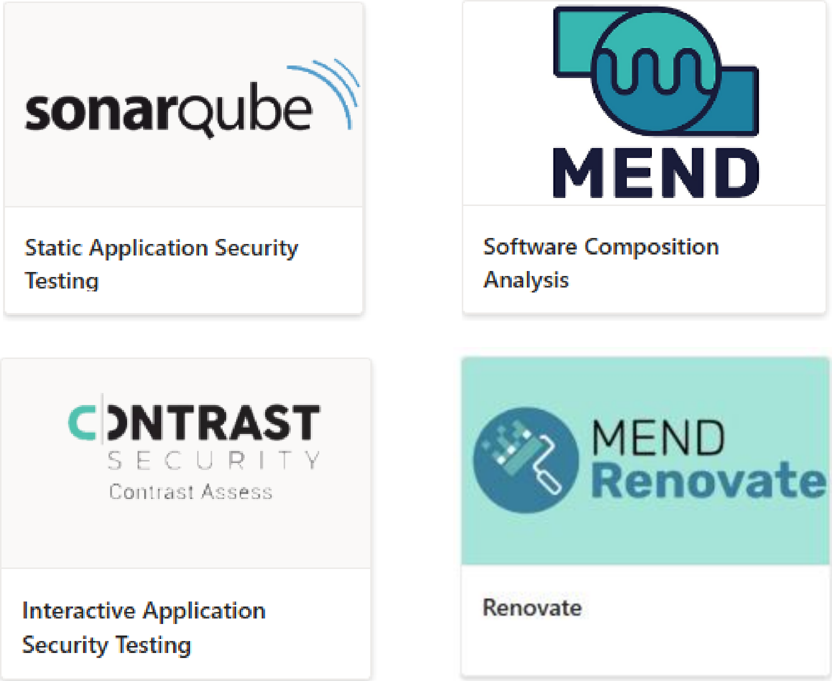
- Perform vulnerability assessment
- Secure architecture review
- Manual security testing
- Automatic security testing
- Document the vulnerability assessment
- (3rd) Keep the portfolio under control and updated

Deploy

- PEN test
- Monitoring infrastructure
- Conduct final security report
- Security review
- (3rd) Portfolio settled according to guidelines

* (3rd) refers to third-party components integrated into our products

Automatic quality gates and security tooling



Static Application Security Testing

Software Composition Analysis

Interactive Application Security Testing

Renovate

How Unit4 ensures CIA robustness at organizational level

Continuous update of standards

- Security teams led by the CISO continually review the Unit4 Information Security Management System (ISMS).
- This ISMS is certified to ISO27001, ISO27017, implemented using the ISO 27002:2022 guidelines.
- Unit4 also holds SOC1 and SOC2 which is audited annually in collaboration with our audit partner (KPMG).
- The Management Framework is further certified to cover Quality with ISO9001.
- The ISMS is compliant with for example GDPR, EU AI ACT, NIS2, DORA and EBA.
- The framework covers the regulations for the use of AI tools internally and in the product.
- Unit4 Global Security Governance Framework applies to all functions of Unit4.
- Link to Unit4's cloud security certifications: https://community4u.unit4.com/cloud/documentation

Builds on secure platforms and with sharp tools and routines

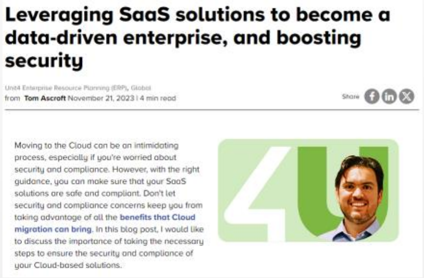
- Microsoft Azure
- Strong SDLC and DevSecOps in development and in production, and investment in great products (MEND, Contrast, Sentinel etc)

Invests in people, security awareness and knowledge

- Training and testing of knowledge
- Regular rehersals and drills on exceptions, disasters and routines
- Unannounced phishing tests and mandatory security training including social hacking awareness

Want to learn more?

Hear it from our CISO in this blog: **Leveraging SaaS solutions to become a data-driven enterprise, and boosting security**



Leveraging SaaS solutions to become a data-driven enterprise, and boosting security

Unit4 Enterprise Resource Planning (ERP), Global
from **Tom Ascroft** November 21, 2023 | 4 min read

Moving to the Cloud can be an intimidating process, especially if you're worried about security and compliance. However, with the right guidance, you can make sure that your SaaS solutions are safe and compliant. Don't let security and compliance concerns keep you from taking advantage of all the **benefits that Cloud migration can bring**. In this blog post, I would like to discuss the importance of taking the necessary steps to ensure the security and compliance of your Cloud-based solutions.

For ERP customers:
AI-Powered ERP: Shaping Businesses of Tomorrow
Webinar from Sept 5 – watch on-demand

Learn more on Unit4 AI
Explore Our AI Philosophy: Visit Unit4.com and read our AI whitepaper.

Additional resources:
Watch this on-demand webinar with Microsoft: **How the Cloud is changing security** and the Unit4 and Microsoft partnership

Read our Unit4 Data Security and Privacy

Q&A

Thank you

for your time and for listening.

Reach out to your Account Manager for next steps.