

CISSP har 8 domæner:

1. **Security and Risk Management**

Defines security goals and objectives, risk mitigation, compliance, business continuity and the law.

Et eksempel: hvis loven ændrer sig i forhold til GDPR, så skal man opdatere sine retningslinjer og genopnå “compliance”.

1. **Asset Security**

Secures digital and physical assets. It’s also related to the storage, maintenance, retention and destruction of data.

Et eksempel: Du skifter hardware og den gamle hardware(hardisk) indeholder kreditkort informationer. Hvordan får du permanent slettet det?

1. **Security Architecture and Engineering**

Optimizes data security by ensuring effective tools, systems and processes are in place.

Et eksempel: Konfigurer en firewall.

1. **Communications and Network Security**

Manage and secure physical networks and wireless communications.

Et eksempel: Hvilken adgang har et “Wireless Hotspot” til dit system og hvem har adgang til det?

1. **Identity and Access Management**

Keeps data secure, by ensuring users follow established policies to control and manage physical assets , like office spaces - and logical assets, such as networks and applications.

Et eksempel: At have et generelt overblik over, hvem der har adgang til hvad og validere, at det er de rigtige individer med den rigtige adgang. Køkkenpersonalet skal ikke have adgang til din serverpark etc. – Men ligeledes skal de heller ikke have adgang til dit datasystem.

1. **Security Assessment and Testing**

Conducting security control testing, collecting and analysing data and conducting security audits to monitor for risks, threats and vulnerabilities.

Et eksempel: Adgang til GDPR informationer. Det kan være bade data-ansvarlig, men også hvem, der skal have adgang til fx. løninformationer.

1. **Security Operations**

Conducting investigations and implementing preventive measures.

Et eksempel: Når IT-afdelingene sender “test phising”-emails ud for at se, om folk kommer til at trykke på links i dem. Dette kan bruges(gerne uden at udstille personalet) til at vise, hvordan hackere forsøger at skaffe sig adgang.

Det kan også være, hvis et device udefra får adgang til dit netværk.

1. **Software Development Security**

Uses secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.

Et eksempel: Hvordan bliver passwords opbevaret? Hvordan gemmer vi data?