WATCHCOM
A COMBITECH COMPANY

Berit Bekkevold

Senior Information Security Consultant

HVORDAN BRUKE RAMMEVERKENE I ANSKAFFELSES-PROSESSEN

Om smarte krav og helhetlig tilnærming til leverandørkjeden

ANGREP PÅ LEVERANDØRKJEDEN SKJER

REUTERS®

World Business Markets Sustainability Legal Breakingviews Technology Investi

Technology

Analysis: MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts

By **Raphael Satter** and **Zeba Siddiqui**

August 8, 2023 10:18 PM GMT+2 · Updated 17 days ago

WATCHCOM
A COMBITECH COMPANY

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

A supply chain attack on a business partner of semiconductor giant Applied Materials will cost the company $250 million in the coming quarter. The company did not specify which partner was hit by the ransomware attack, but said that the incident would disrupt upcoming shipments.

3CX's supply chain attack was caused by... another supply chain attack

Carly Page @carlypage_ / 2:00 PM GMT+2 • April 20, 2023

OGSÅ HER HJEMME…

– Vi har avdekket en hittil ukjent sårbarhet i programvaren til en av våre leverandører. Denne sårbarheten er utnyttet av en ukjent aktør. Vi har nå lukket denne sårbarheten.

Departementer utsatt for dataangrep:

Angriperne utnyttet hittil ukjent sårbarhet

WATCHCOM
A COMBITECH COMPANY

DETTE SIER RAPPORTENE

- Enisa Threat landscape 2022:

In 2022, the most common initial attack vectors were compromised credentials at 19% of breaches, phishing at 16% of breaches, cloud misconfiguration at 15% of breaches and vulnerability in third-party software at 13% of breaches. The 2021 report saw the same order of the top four initial attack vectors.

19%

of breaches occurred because of a compromise at a business partner.

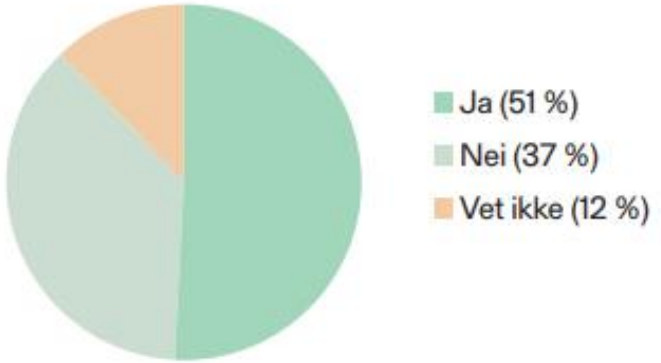
45%

of the breaches were cloud-based.

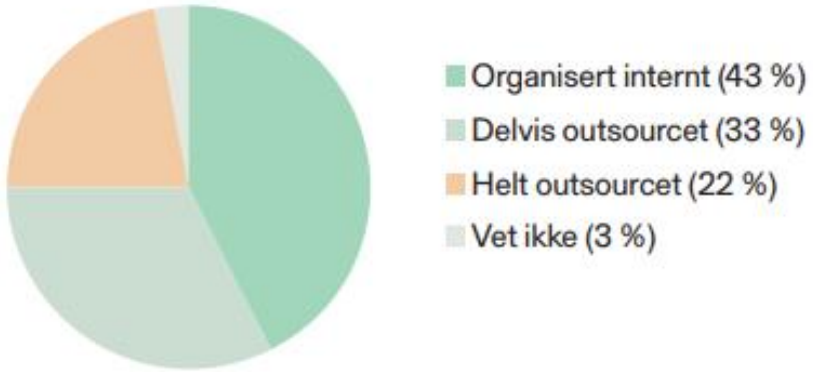
DETTE SIER RAPPORTENE

- NSRs Mørketallsundersøkelse 2022

Figur 2. Har virksomheten et rammeverk og/eller styringssystem for informasjonssikkerhet? Total sample; base n = 2500



Figur 1. Er virksomhetens it-drift organisert ved at den er helt outsourcet, delvis outsourcet eller er all drift organisert internt? Total sample; base n = 2500



WATCHCOM
A COMBITECH COMPANY

ISO/IEC 27001

Contents

Page

Foreword ... iv
Introduction ... v
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 1
4 Context of the organization ... 1
4.1 Understanding the organization and its context ... 1
4.2 Understanding the needs and expectations of interested parties ... 1
4.3 Determining the scope of the information security management system ... 2
4.4 Information security management system ... 2
5 Leadership ... 2
5.1 Leadership and commitment ... 2
5.2 Policy ... 3
5.3 Organizational roles, responsibilities and authorities ... 3
6 Planning ... 3
6.1 Actions to address risks and opportunities ... 3
6.1.1 General ... 3
6.1.2 Information security risk assessment ... 4
6.1.3 Information security risk treatment ... 4
6.2 Information security objectives and planning to achieve them ... 5
7 Support ... 6
7.1 Resources ... 6
7.2 Competence ... 6
7.3 Awareness ... 6
7.4 Communication ... 6
7.5 Documented information ... 6
7.5.1 General ... 6
7.5.2 Creating and updating ... 7
7.5.3 Control of documented information ... 7
8 Operation ... 7
8.1 Operational planning and control ... 7
8.2 Information security risk assessment ... 8
8.3 Information security risk treatment ... 8
9 Performance evaluation ... 8
9.1 Monitoring, measurement, analysis and evaluation ... 8
9.2 Internal audit ... 8
9.2.1 General ... 8
9.2.2 Internal audit programme ... 9
9.3 Management review ... 9
9.3.1 General ... 9
9.3.2 Management review inputs ... 9
9.3.3 Management review results ... 9
10 Improvement ... 10
10.1 Continual improvement ... 10
10.2 Nonconformity and corrective action ... 10
Annex A (normative) Information security controls reference ... 11
Bibliography ... 19

Annex A
(normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.

Table A.1 — Information security controls

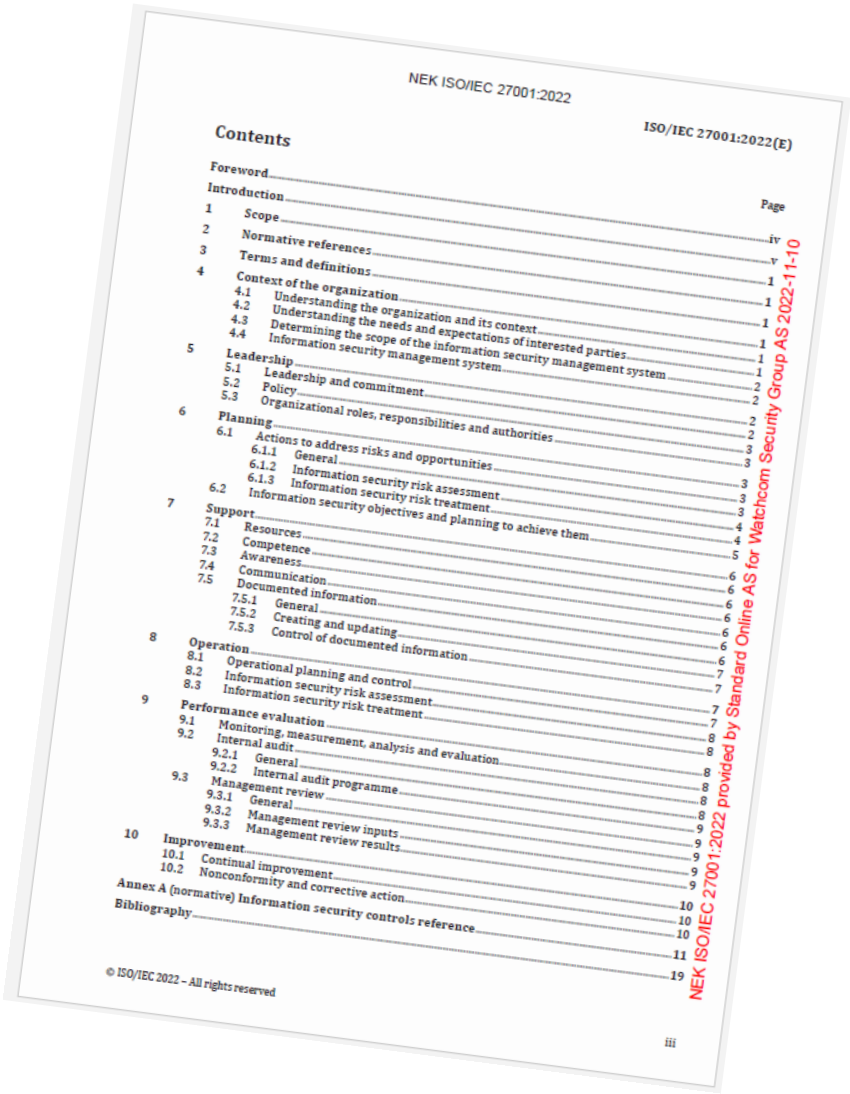
5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.
	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
	Contact with special interest groups	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
	ıformation security in project anagement	**Control** Information security shall be integrated into project management.
	ventory of information and ıer associated assets	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.
	ptable use of information other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
	n of assets	**Control** Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

WATCHCOM
A COMBITECH COMPANY

ISO/IEC 27001

- Clause 8.1: The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are **controlled**.
- Annex A

5.19	Information security in supplier relationships	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
5.20	Addressing information security within supplier agreements	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review and change management of supplier services	**Control** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.


NEK ISO/IEC 27001:2022

ISO/IEC 27001:2022(E)

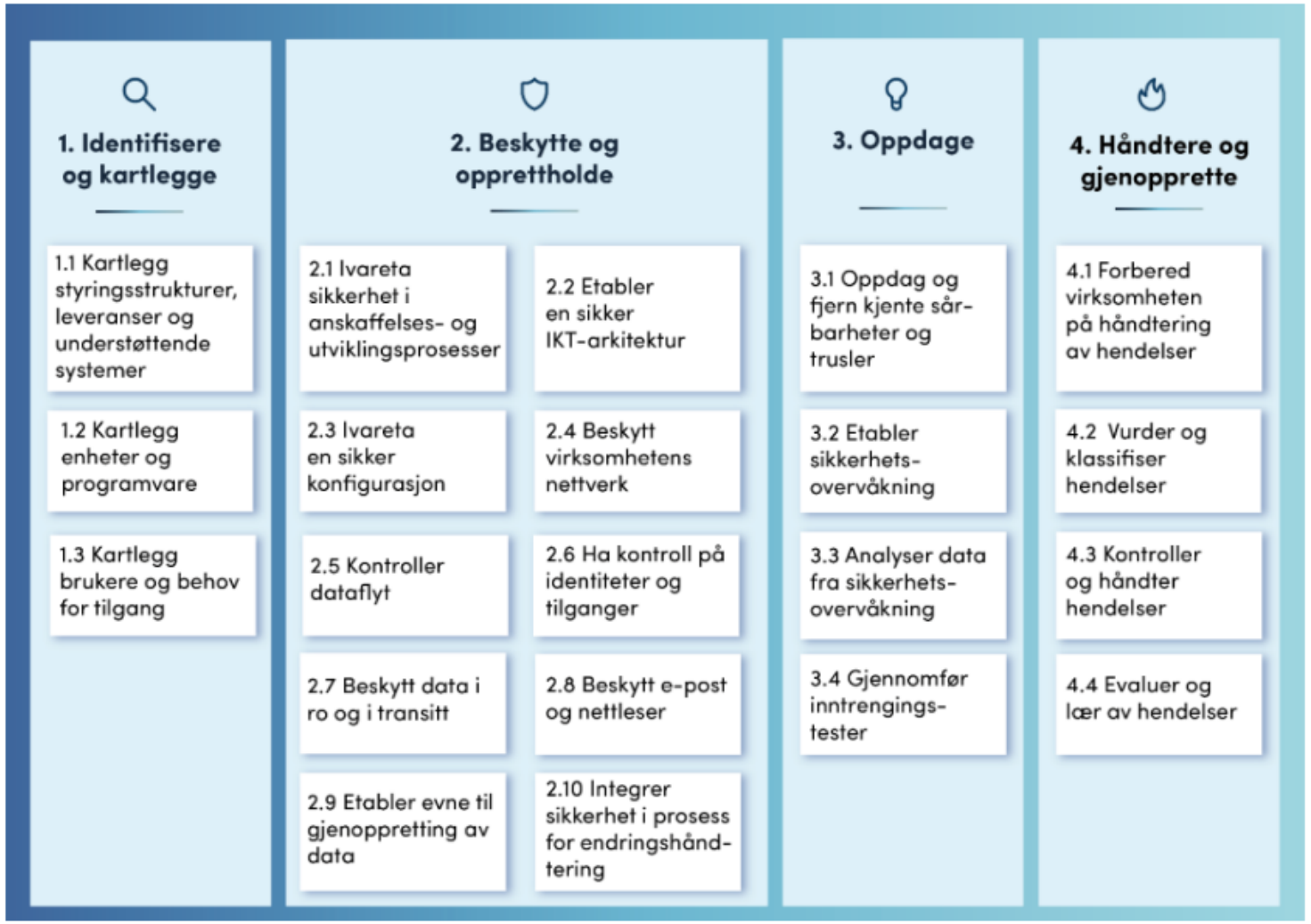
Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Context of the organization 1
4.1 Understanding the organization and its context 1
4.2 Understanding the needs and expectations of interested parties 1
4.3 Determining the scope of the information security management system 1
4.4 Information security management system 2
5 Leadership 2
5.1 Leadership and commitment 2
5.2 Policy 2
5.3 Organizational roles, responsibilities and authorities 3
6 Planning 3
6.1 Actions to address risks and opportunities 3
6.1.1 General 3
6.1.2 Information security risk assessment 3
6.1.3 Information security risk treatment 3
6.2 Information security objectives and planning to achieve them 4
7 Support 4
7.1 Resources 5
7.2 Competence 6
7.3 Awareness 6
7.4 Communication 6
7.5 Documented information 6
7.5.1 General 6
7.5.2 Creating and updating 6
7.5.3 Control of documented information 7
8 Operation 7
8.1 Operational planning and control 7
8.2 Information security risk assessment 8
8.3 Information security risk treatment 8
9 Performance evaluation 8
9.1 Monitoring, measurement, analysis and evaluation 8
9.2 Internal audit 8
9.2.1 General 8
9.2.2 Internal audit programme 9
9.3 Management review 9
9.3.1 General 9
9.3.2 Management review inputs 9
9.3.3 Management review results 10
10 Improvement 10
10.1 Continual improvement 10
10.2 Nonconformity and corrective action 11
Annex A (normative) Information security controls reference 19
Bibliography

WATCHCOM
A COMBITECH COMPANY

NSM GRUNNPRINSIPP FOR IKT-SIKKERHET 2.0



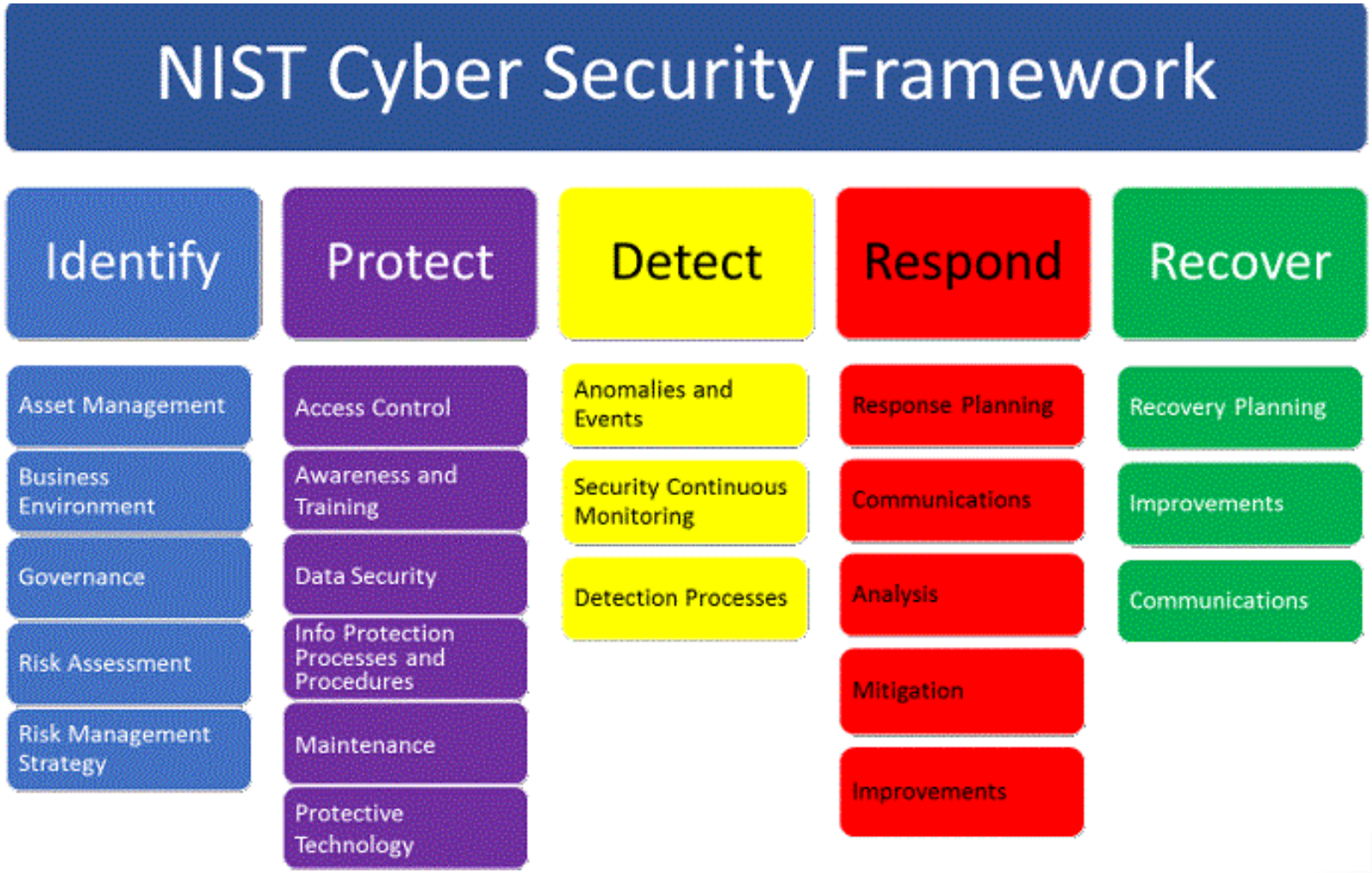
WATCHCOM
A COMBITECH COMPANY

NSM GRUNNPRINSIPPER FOR IKT-SIKKERHET 2.0

- 2.1 - Ivareta sikkerhet i anskaffelses- og utviklingsprosesser. IKT-produkter og IKTtjenester med svak sikkerhet kan øke sårbarheten og redusere sikkerhetsnivået i IKT-systemet
- 2.1.1: Integrer sikkerhet i virksomhetens prosess for anskaffelser. Fastsett krav til IKT-sikkerhet ved anskaffelse av alle IKT-produkter og IKT-tjenester,
- 2.1.4 Reduser risiko for målrettet manipulasjon av IKT-produkter i leverandørkjeden
- 2.1.9 Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
- 2.1.10 Undersøk sikkerheten hos tjenesteleverandør ved tjenesteutsetting
- 2.2 - Etabler en sikker IKT-arkitektur. Inkluder sikkerhet i hele livsløpet fra anskaffelse til avhending.

WATCHCOM
A COMBITECH COMPANY

NIST CSF


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

NIST CYBERSECURITY FRAMEWORK

- ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
- ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

ANSKAFFELSESPROSESSEN

1. Gjør en risikovurdering av prosessen
2. Bruk tiltaksplanen til å identifisere behovet og må/bør-krav
3. Bruke kjente rammeverk for å sikre helhetlig tilnærming
4. Bruk smarte krav for å sikre tydelige krav og en forutsigbar prosess

DEFINER KRAVENE

- **S**pecific
- **M**easurable
- **A**chievable
- **R**elevant
- **T**imely

EKSEMPEL

Krav	Må/bør	dokumentasjon	Kriterier	Vurdering
Leverandøren har et styringssystem i tråd med ISO 27001, NIST CSF, NSM GP 2.0 e-l	Må	ISO IEC 27001 Sertifikat m omfangsdokument og policy, revisjonsrapport	Framlagt sertifikat, omfangsdokument inkluderer tjenestene som skal anskaffes	10
Leverandøren har en oversikt over hvem som skal ha innsyn i virksomhetens informasjon	Må	Prosedyrer for tilgangsstyring av virksomhetens informasjon, rutine for taushetserklæringer og liste over ansatte med tilgang.	Oppdaterte Prosedyrer for tilgangsstyring	10
Leverandøren skal ha rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering.	Bør	Beredskapsplaner og rutiner for avvikshåndtering	Beredskapsplan i tråd med iso/iec 27001 beskriver hendelser relevant for tjenesten	7

FØLG OPP LEVERANDØRENE

- Gjennomgå krav og kriterier for godkjenning med jevne mellomrom
- Avtal og hold regelmessige møter med leverandørene om informasjonssikkerheten
- Innhent målingsresultater og revisjonsrapporter fra leverandørene og bruk dem i eget styringsarbeid
- Inviter leverandørene til beredskapsøvelser!


WATCHCOM
A COMBITECH COMPANY

WATCHCOM

A COMBITECH COMPANY

WATCHCOM.NO

COMBITECH.SE | .FI | .DK | .COM