



# Supplier Risk Management @ ASML

Janneke Schepers/ Robbert Kramer

Director Analytics & Business Support  
Strategic Sourcing & Procurement, ASML

19 april 2018, Vianen

# Challenge in Information Security

ASML

Public  
Slide 2  
April, 2018



**Ever increasing computing power is to the security of the connected world as the invention of gun powder to the city wall.**

# ASML in 34 years



- 0% market share
- Employees: 31
- Locations: 2 (NL, US)
- Sales: € 1,2 million
- R&D: € <5 million

- Employees: > 19.000, 115 nationalities
- Locations: 60, in 16 countries
- Sales: € 9,053 billion (end 2017)
- R&D: € 1,260 billion (end 2017)



# ASML develops & makes machines that make chips

That's a 100-ton, €95-mln precision instrument with >100,000 components

**ASML**

Public  
Side 4  
April, 2018



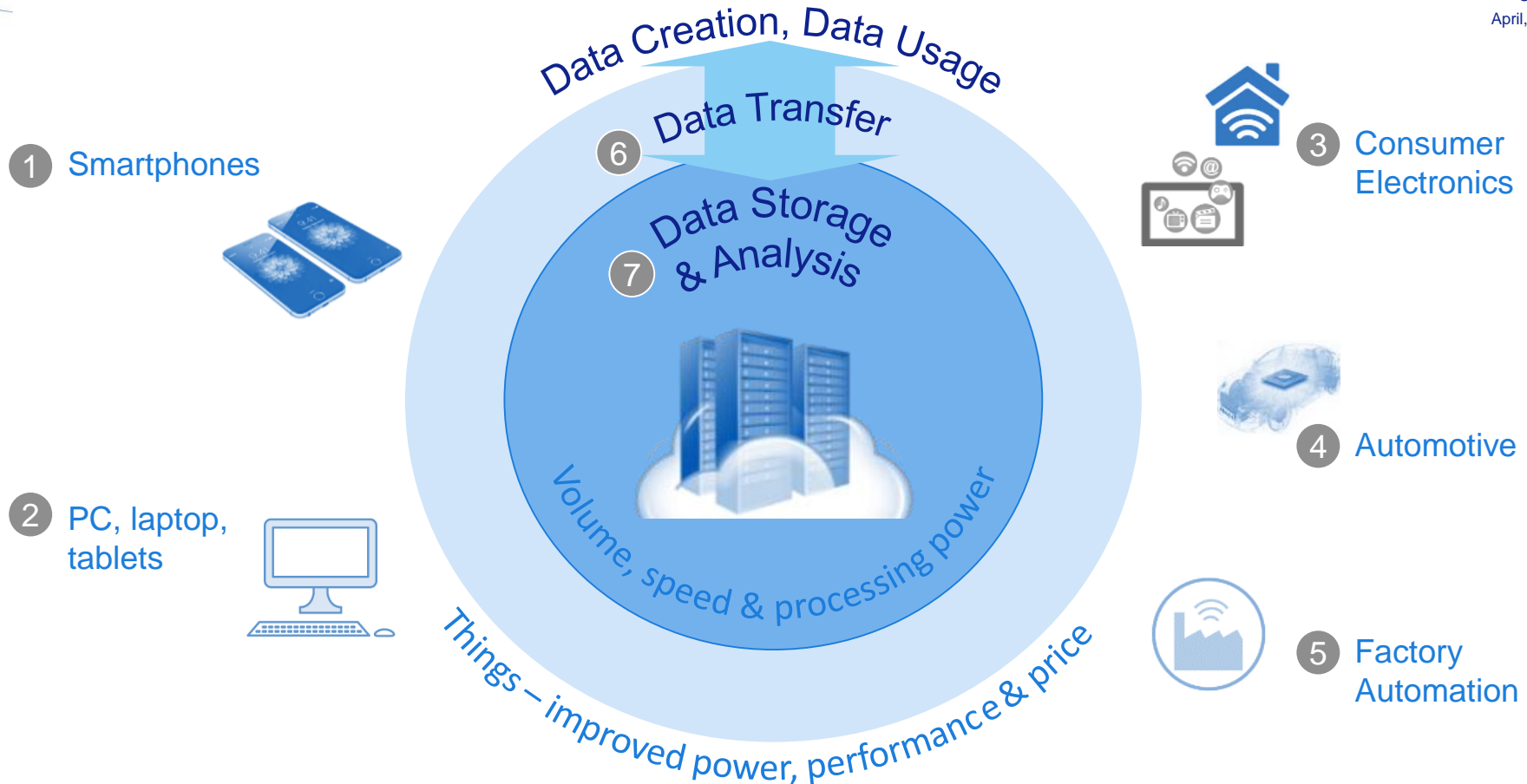
*We manage to  
make this work*



# ASML market is driven by the digital revolution

ASML

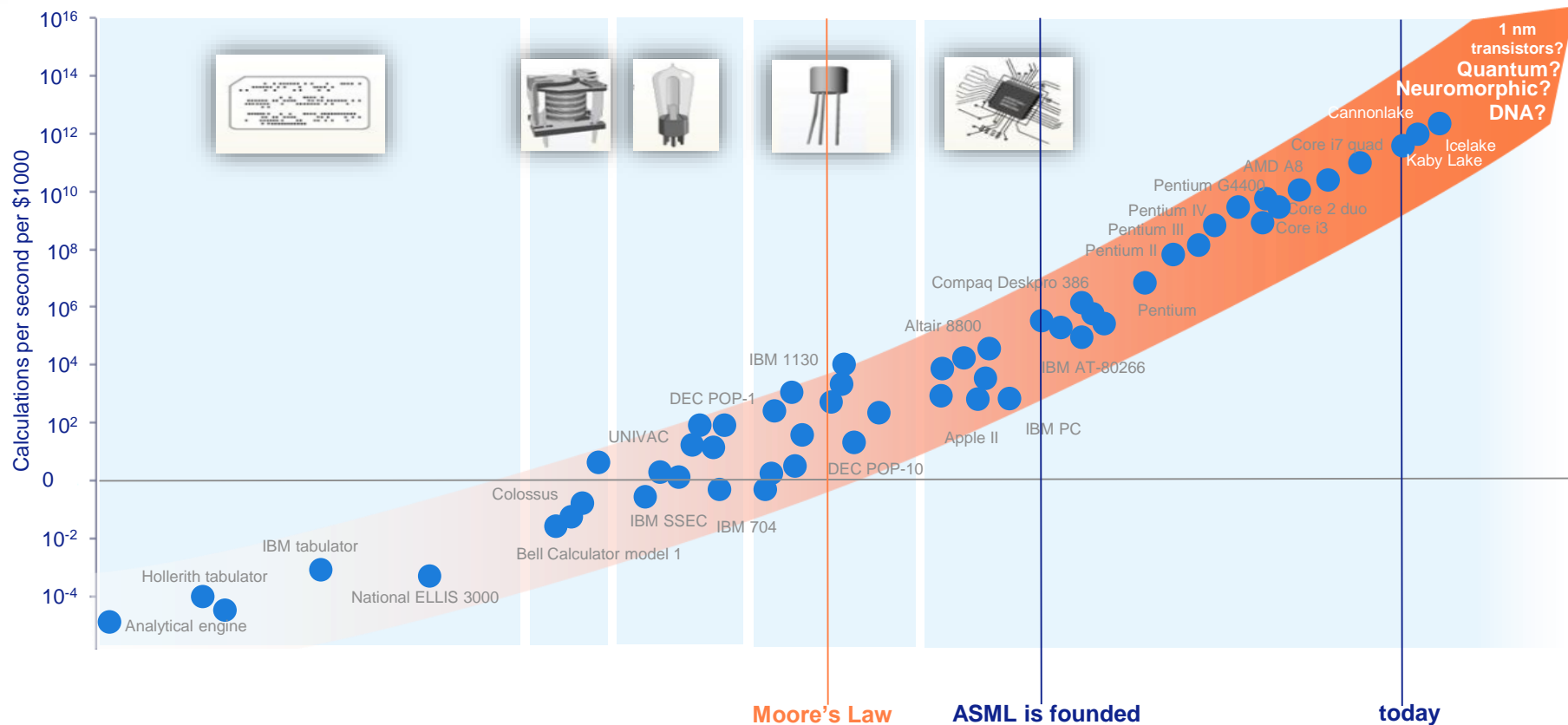
Public  
Slide 5  
April, 2018



# Moore's Law of economics drives computing power

ASML

Public  
Slide 6  
April, 2018

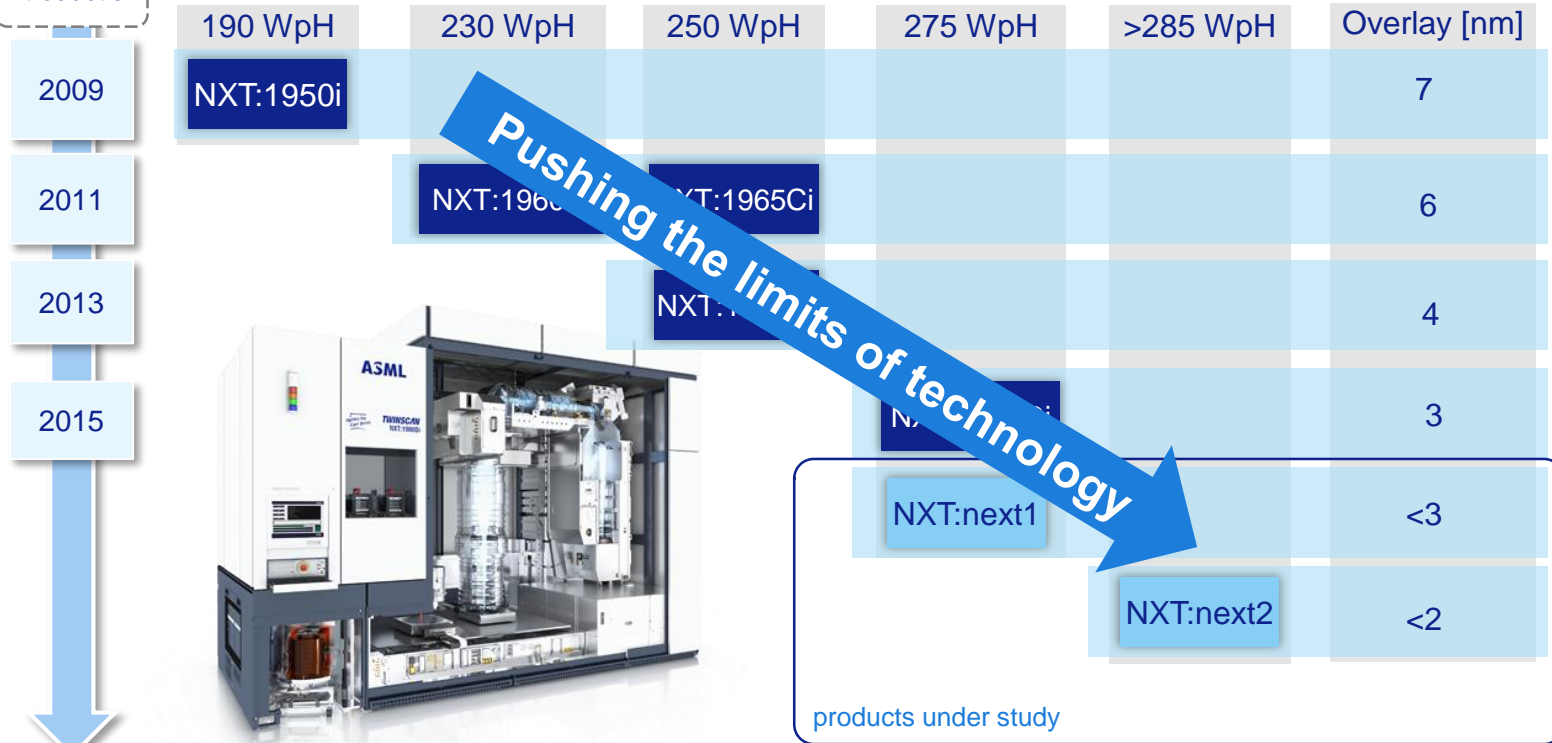


# To deliver on Moore's law, we push technical limits

ASML

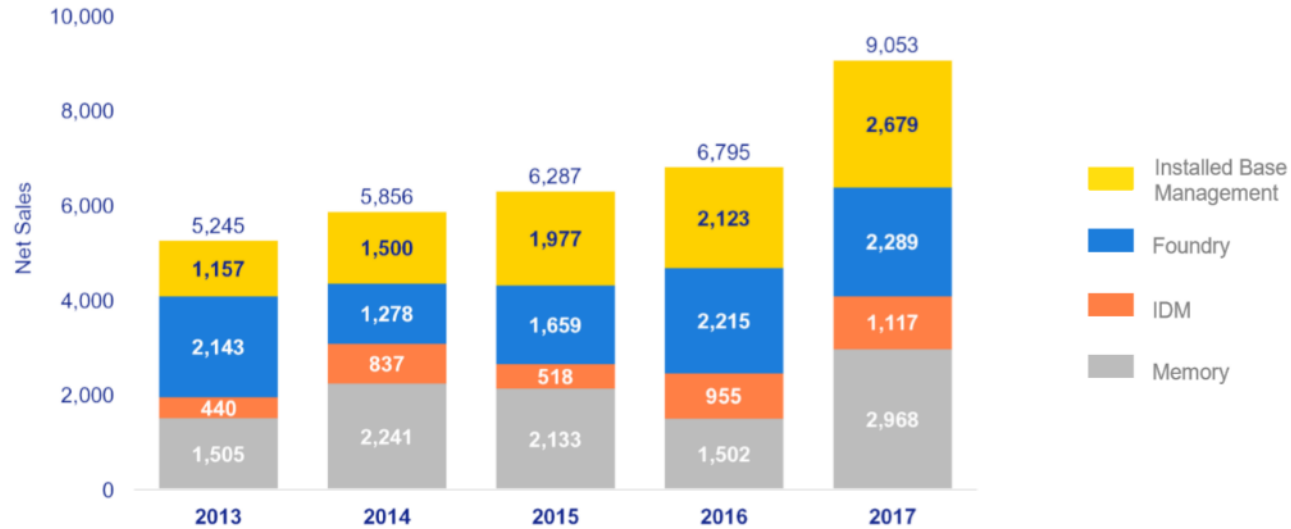
Public  
Slide 7  
April, 2018

introduction



# Financial report 2017

## Total net sales million € by End-use



Installed Base Management equals our service and field option sales

SOURCE: [https://staticwww.asml.com/doclib/investor/financial\\_results/2018/asml\\_20180107\\_presentation.pdf](https://staticwww.asml.com/doclib/investor/financial_results/2018/asml_20180107_presentation.pdf)

All disclaimers pertaining to forward looking statements as documented in reference apply



# Sustainable relationship with suppliers

ASML

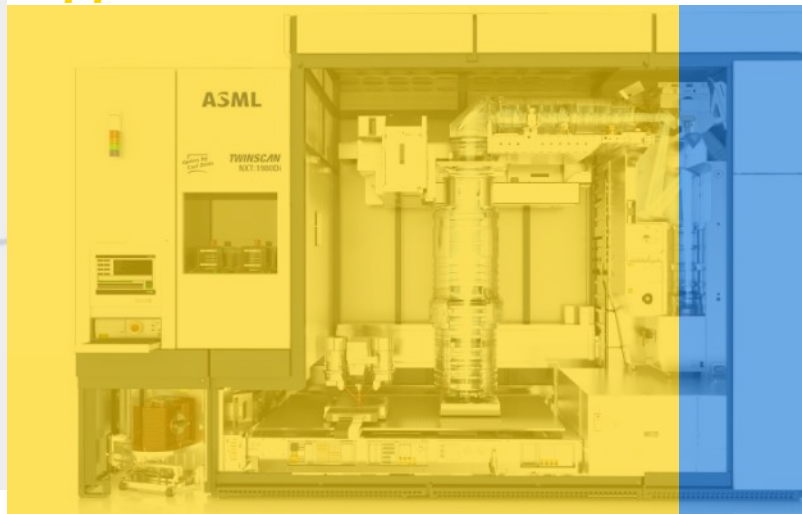
Public  
Slide 9  
April, 2018

## Sustainable relationship with suppliers

Key to our success is our ability to build a world-class supplier network that enables us to concentrate on our core strengths and enables our suppliers to gain fair benefits from working with us.

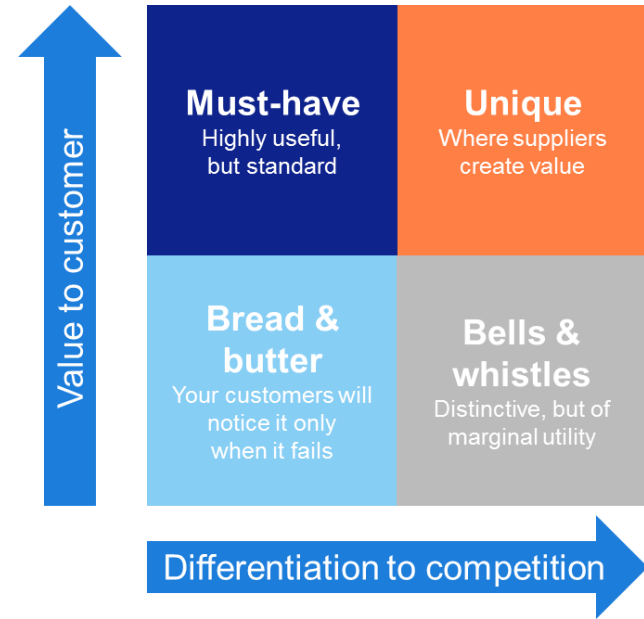
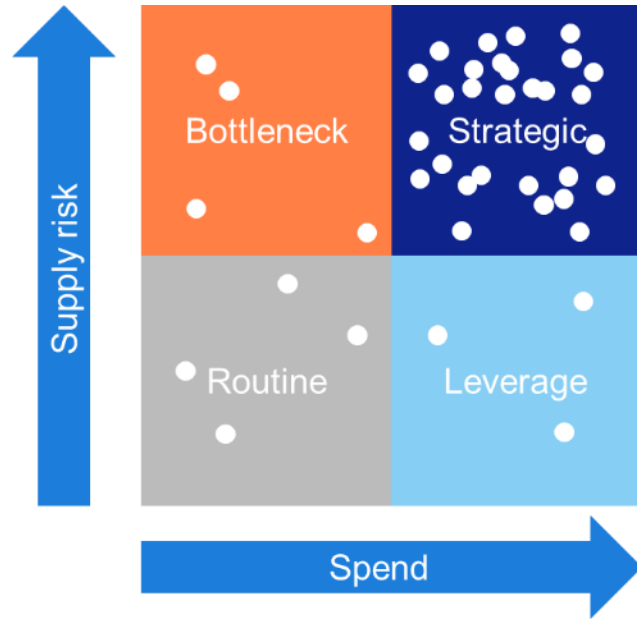
*suppliers*

**ASML**



**Up to 85% of our systems is procured**

# Our sourcing model is not the classic Kraljic matrix

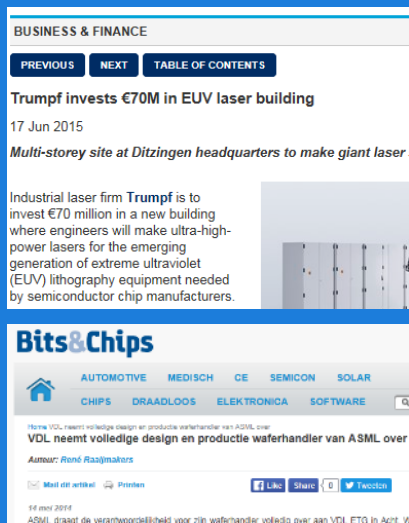


# We have very close ties with our suppliers

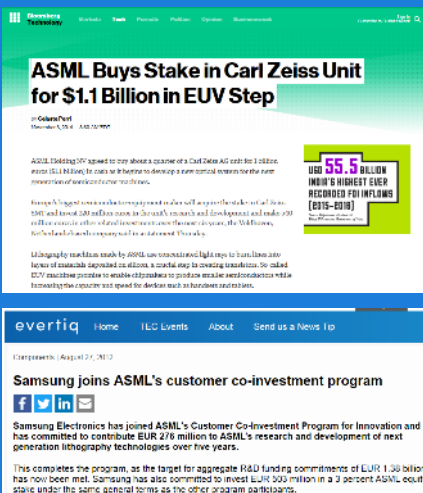
ASML

Public  
Slide 11  
April, 2018

From  
shared responsibility

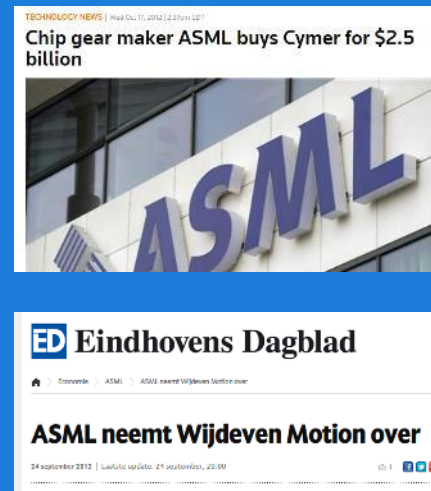


To  
part ownership



As our customers have  
a stake in ASML

To  
full ownership



# What drives value for our customers?

MAKE IT  
**WORK**

Execute the roadmaps

MAKE IT  
**WELL**

Deliver quality products and services

MAKE IT  
**TOGETHER**

Align customers, suppliers and peers

MAKE IT  
**WORTH IT**

Improve cost per function /  
return on investments

MAKE US  
**GROW**

Develop our people and processes

# ASML risk management up to 2 years ago

## QLTCS Supplier Profile

Q1	L1	T1	C1	S1	Compliance
Q2	L2	T2	C2	S2	Business Continuity
Q3	L3	T3	C3	S3	Environmental Performance
Q4	L4	T4	C4	S4	Health & Safety Performance
Q5	L5	T5	C5	S5	Labor Ethics
Q6	Yield	T6	C6	S6	Business Ethics
Q7	Suppl	T7	C7	S7	IP Protection / Information Security
			C8	S8	Supplier Management (N-tier, Sustainability)

## Yearly Risk Assessment

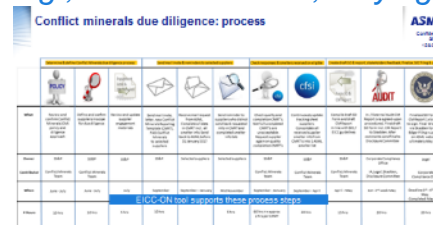
Risk aspect
<b>Strategic Risks</b>
Single source
Customer portfolio
Technology Ownership
Virtual Integration level
Material availability
2nd tier management
Flexibility Requirement
IP Protection
<b>Natural Hazards and Calamities</b>
Natural Hazards
Equipment/utilities risk
<b>Financial Risk</b>

## Financial Risk Assessment



## Multiple others, some ad hoc

*E.g., conflict minerals, varying scope*



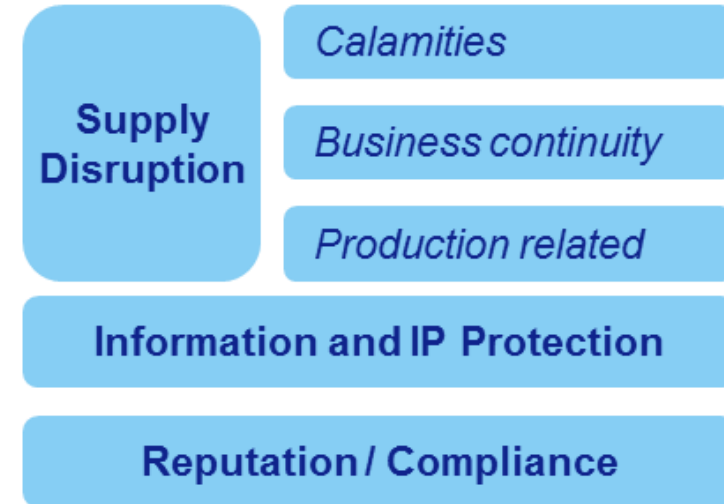
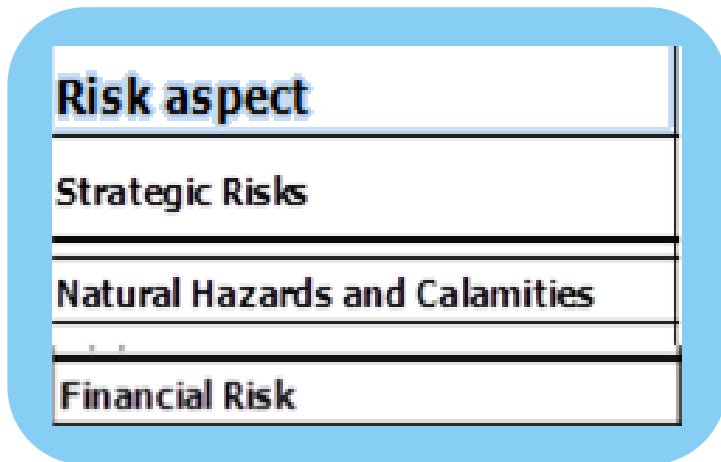
Risk information of suppliers was scattered. Instruments were partially overlapping.  
The risk management process was annual rather than continuous.



# Risk Profiling will focus on the core risk domains

From 3 risk aspects

To 4 risk domains



*... of which strategic risks harbors a mix of cost, IP and disruption risks*

*providing clarity on those risks deemed relevant in ASML risk universe*

# Process is captured in a single tool

ASML

Public  
Slide 15  
April, 2018

43% of data input  
is automated



Financial expert  
ratings

Global risk indicators  
by Maplecroft

Supplier profile scores

Vendor master- and  
contract data

Sourcing Lead completes  
assessment

Country	Supplier	Risk	Assessment	Score	Comments
USA	Supplier A	High	Assessment completed	100	Assessment completed
USA	Supplier B	Medium	Assessment completed	80	Assessment completed
USA	Supplier C	Low	Assessment completed	60	Assessment completed
USA	Supplier D	High	Assessment completed	100	Assessment completed
USA	Supplier E	Medium	Assessment completed	80	Assessment completed
USA	Supplier F	Low	Assessment completed	60	Assessment completed
USA	Supplier G	High	Assessment completed	100	Assessment completed
USA	Supplier H	Medium	Assessment completed	80	Assessment completed
USA	Supplier I	Low	Assessment completed	60	Assessment completed
USA	Supplier J	High	Assessment completed	100	Assessment completed

Ownership,  
dependency

Intellectual property  
ownership

Legal, compliance

Recovery times

Category Manager  
reviews risks & plans

Risk Domain	Indicator
SUPPLY DISRUPTION	
Decision(s)	
Risk #	Indicator
L G1	Ownership / management stability assessment

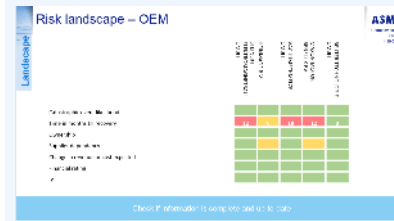
Sourcing Lead drafts  
plans with experts

Finance

Legal

CIP

Standard reporting incl.  
red flags in place



SS&P staff ensure  
decision making is in line  
with agreed governance



# Process is based on a preliminary governance model

**Process map with  
RACI has been drafted**

**The main supplier  
risk domains are in scope**

**Rules defined to escalate risks to  
the appropriate management levels**

*the governance model is confidential  
and therefore not part of this hand-out*

- A process map with RACI has been drafted and is embedded into the Procurement process framework
- Risk review meetings will be scheduled

- 6 risk domains are assessed – calamities, financial stability, ownership, IP ownership, information security and compliance
- Typical mitigative responses are commercial interventions or supplier development.

- A risk appetite dialogue sets the threshold for scoping and risk level categorization
- Mitigation plan approval levels based on risk level categorization
- Red flag reports are available per risk domain

# What is expected of suppliers?

## Information Security requirements

### Draft Information Security areas (based on ISO27001:2013)



Information Security  
Management System (ISMS)



Human Resources Security



Access Control



Cryptographic Controls



Physical Security



Operations Security



Logging & Monitoring



Control of Software



Network Security /  
Information Transfer



Network & Mobile Security



Development & Support  
Security



Supplier Information Security



Information Security Incident  
Management



Information Security /  
Business Continuity



Compliance



Information Security Review

# ASML engineering intellectual property is critical

**ASML**

Public  
Slide 18  
April, 2018



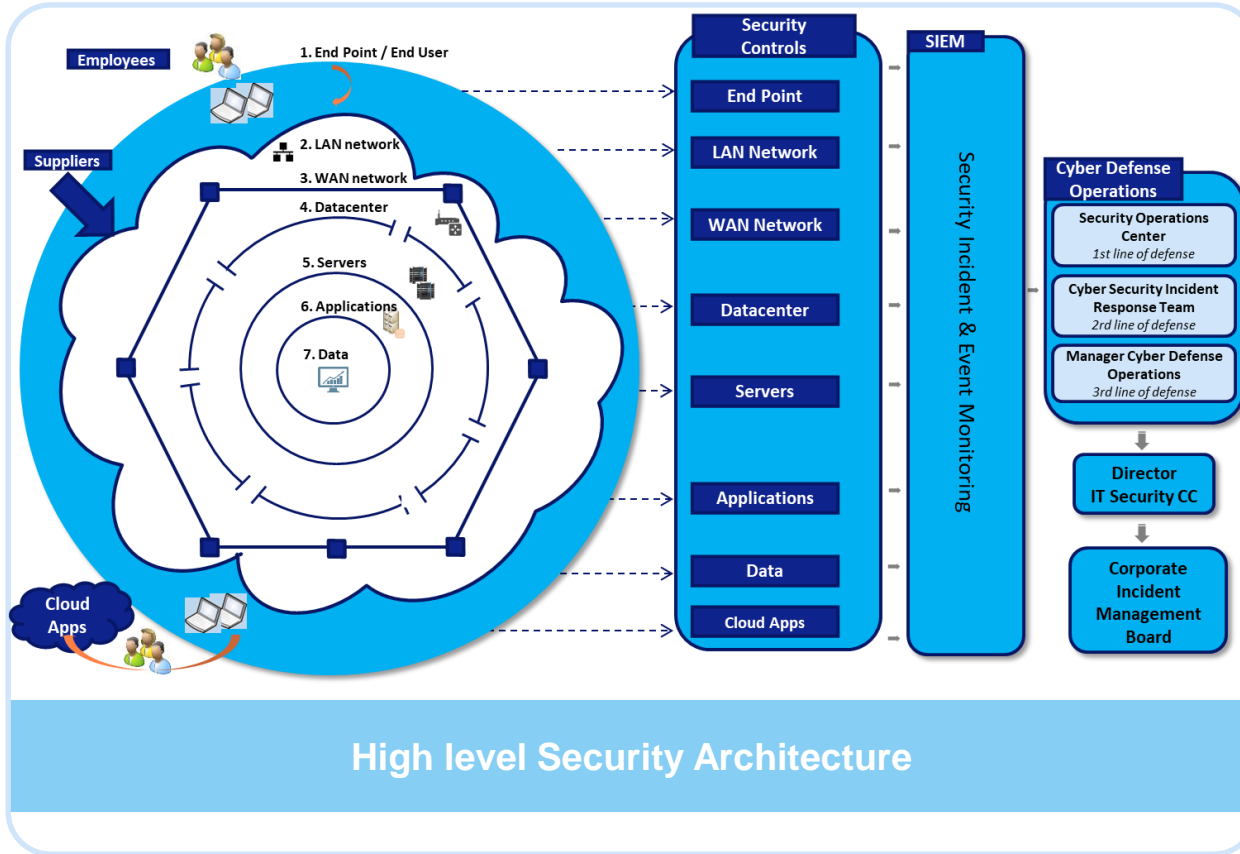
Patent wall at the experience center

## Engineering Top Secrets and IP

- Information exchange is needed
- Work together with supplier on new technology
- New technology can be patented but has to follow IP process



# Security Architecture




**Security Architecture**  
**Layers of defense**  
**Security controls for each layer**

**ASML IT Infrastructure is network level connected with suppliers**

**High privileged suppliers for outsourced activities**

# Inclusion based on impact

ASML engineering intellectual property is critical



Patent wall at the experience center

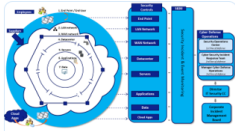
ASML  
July 2018  
April 2018

Engineering Top Secrets and IP

- Information exchange is needed
- Share together with supplier on new technology
- New technology can be patented but has to follow IP process

## (Engineering) Top Secrets

Security Architecture



High level Security Architecture

ASML  
July 2018  
April 2018

Security Architecture

Layers of defense

Security controls for each layer

ASML IT Infrastructure is network level connected with suppliers

High privileged suppliers for outsourced activities

## Network connected suppliers & high privileged

GDPR, Cloud

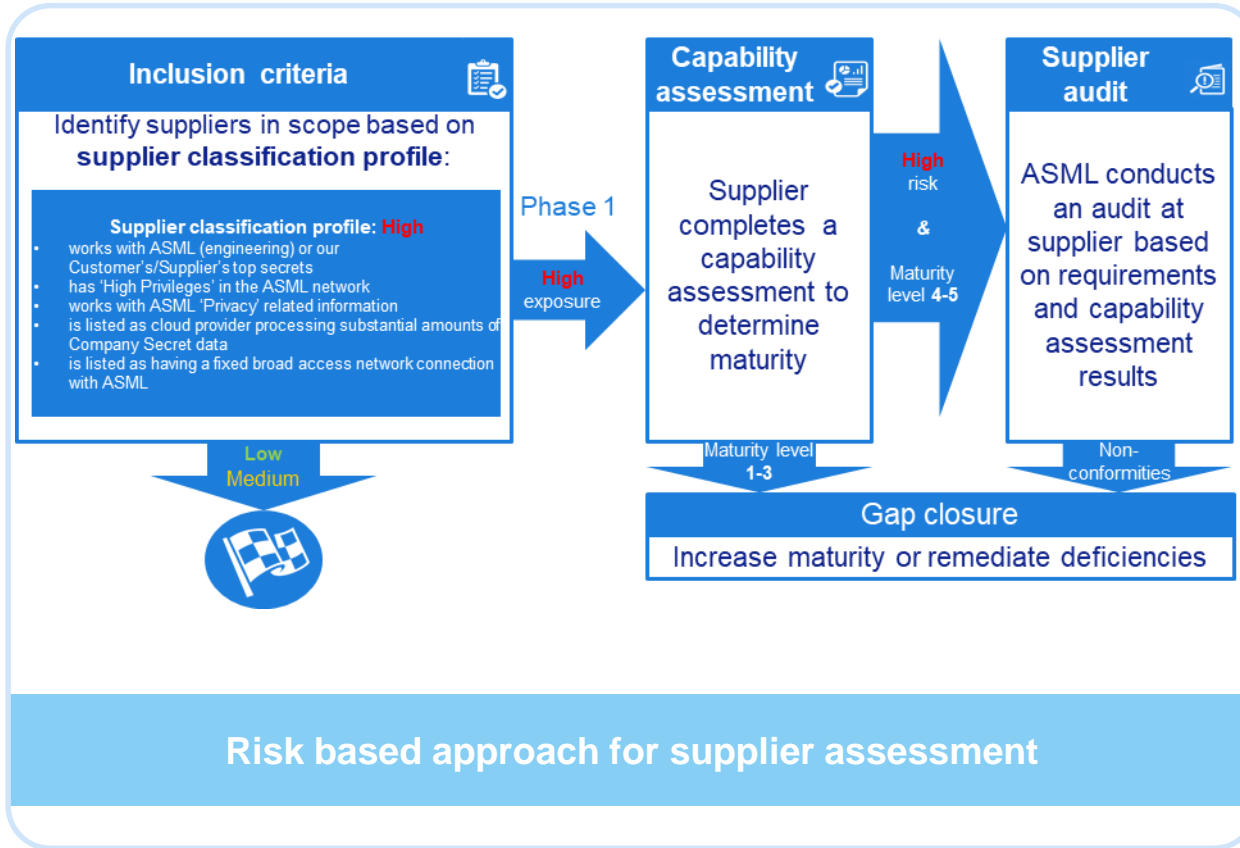


General Data Protection Regulation

ASML

## GDPR and cloud

# Supplier Risk Management



## Supplier Risk Management

- Inclusion of suppliers is risk based
- Questionnaire answered by supplier
- Outcome of questionnaire validated and used for further actions
- Maturity of supplier determines how to proceed

# Information Security survey

**ASML**

## Information Security Management System (ISMS)

Is your company ISO 27001 certified?  
In case your company is not ISO 27001 certified, do you have an information security management system in place according to ISO 27001 or similar standard?

1 ISMS activities are performed ad hoc

2 ISMS activities are performed based on limited guidance and best effort  
Typical evidence: Informal ISMS instructions / guidelines

3 ISMS activities are performed based on defined and documented practices  
Typical evidence: Defined ISMS processes and supporting materials (e.g. risk register for action tracking etc.)

4 ISMS activities are performed based on formal practices that are periodically reviewed and its effectiveness measured  
Typical evidence: Approved and up-to-date ISMS policy (including governance setup) Information Security dashboard (project status, Information Security insight)

5 ISMS activities are performed via an automated GRC solution, the organizations ISMS is certified  
Typical evidence: ISO 27001 certificate

Please indicate your type of evidence:

Conduct your own online surveys

**InfoSec questionnaire based on ISO27001**

## Information Security Survey

- Based on ISO 27001
- First Wave of suppliers selected for deployment
- Cloud application (secure!) for survey management
- SharePoint solution for monitoring outcomes & progress on improvement plans

# Risk levels determines seniority of decision makers

Risk domain	Very low risk (excluded)	Low risk	Medium risk	High risk (red flag)
Calamities	Commodity products with multiple suppliers in the market and short order lead times are excluded from the detailed risk profiling			
Ownership continuity				
Financial stability				
IP ownership				
Information Security		<ul style="list-style-type: none"> <li>Access to critical knowledge, but ISO27001 compliant</li> </ul>	<ul style="list-style-type: none"> <li>Minor non-conformities vs ISO27001</li> <li>Supplies indirect competitors</li> </ul>	<ul style="list-style-type: none"> <li>Major non-conformities vs ISO27001</li> <li>Supplies direct competitors</li> </ul>
Reputation & compliance				

*Typical Highest Approval level*

Category Manager

Sourcing Management

Executive Management





# We continue to invest in our suppliers and people

*Our culture and business sector*



**To contribute to this world of exponential improvement**



**In close relation with suppliers**



**Act now with the future in mind**



**Where supplier development is not just a buzz word – it is a necessity**

*Welcome to our world*

# Selected vacancies at ASML

IT – Quality and Compliance Officer

IT- Application Security Analyst

IT - 3rd party IT Security Manager

<https://www.asml.com/careers/vacancies/en/s32420>

## Some numbers

- Currently 654 vacancies world wide
- Veldhoven 427
- From high school diploma up to PhD
- From student to senior

The image features the ASML logo in a bold, dark blue, sans-serif font. The logo is positioned on the left side of the frame. The background is a light blue gradient with abstract, flowing white lines that create a sense of movement and depth. The lines are more concentrated around the logo and fade out towards the right.

**ASML**