



**Charter
of Trust**

Charter of Trust

on Cybersecurity

Watson IoT centre

November 27, 2018

Welcome and Opening Address – Jonathan Sage
Government and Regulatory Affairs, IBM

charter-of-trust.com | #Charter of Trust

Together with strong partners we signed the “Charter of Trust” – with three important objectives

1. **Engage with policy makers** to collaborate, educate and raise awareness in cyber security
2. **Raise the bar in cyber security** with tangible measures and results
3. **Create a reliable foundation** on which confidence in a networked, digital world can take root and grow

enel

IBM

Munich Security Conference **msec**
Münchner Sicherheitskonferenz

NXP

SIEMENS

 **AES**

AIRBUS

Allianz 

Atos


CISCO

DAIMLER

DELL Technologies

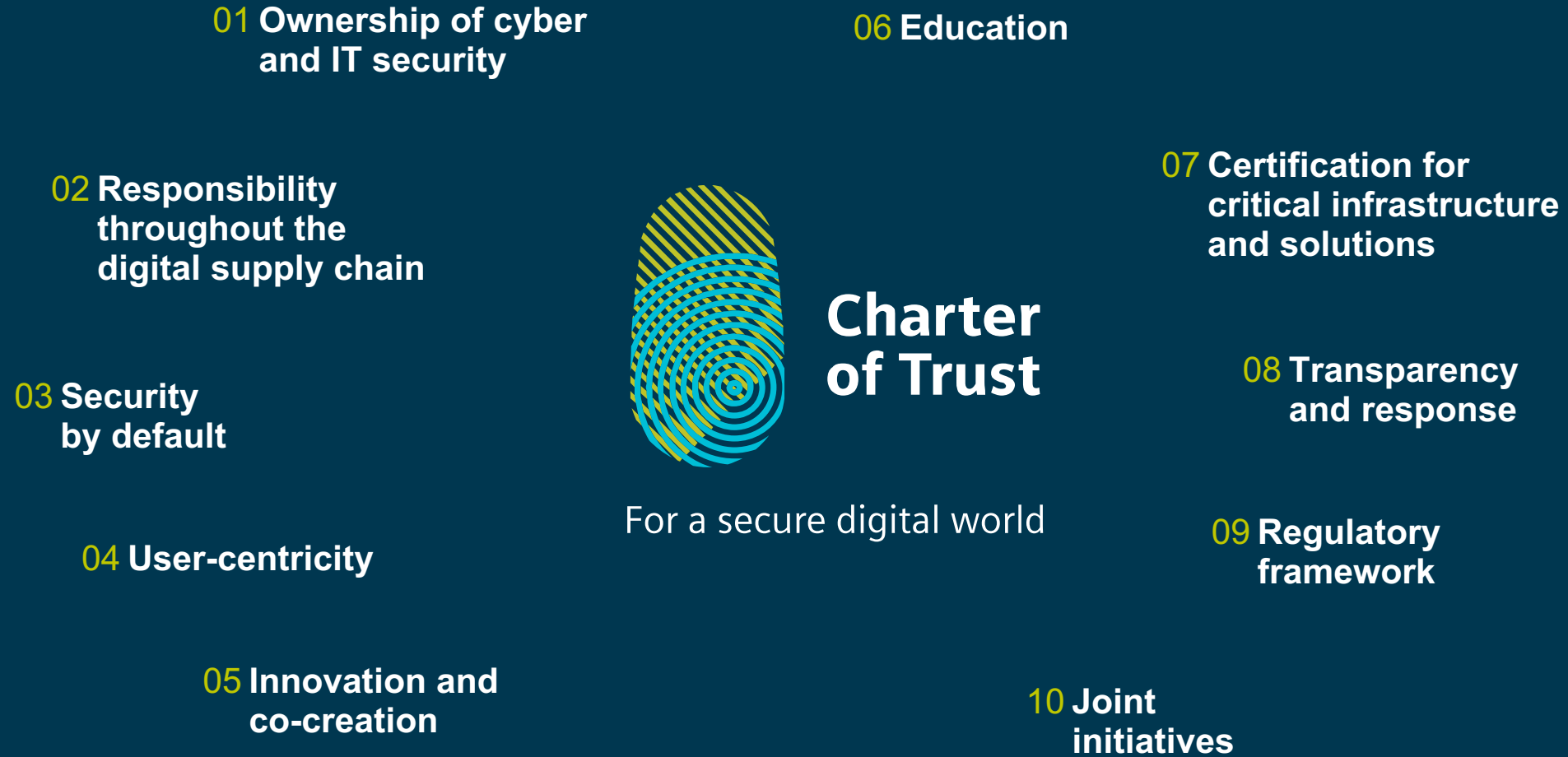
SGS



 **TOTAL**



And we came up with ten key principles





Charter of Trust

charter-of-trust.com

Together we strongly believe that ..

- Effective cybersecurity is a precondition for an open, fair and successful digital future
- By adhering to and promoting our principles, we are creating a foundation of trust for all

As a credible and reliable voice, we collaborate with key stakeholders to achieve trust in cybersecurity for global citizens.



Charter
of Trust

IBM believes organizations that collect, store, manage or process data have an obligation to handle it responsibly.

That belief – embodied in our century-long commitment to trust and responsibility in all relationships – is why the world's largest enterprises trust IBM as a steward of their most valuable data.

We take that trust seriously and earn it every day by following these responsible principles and practices.

Ginni Rometty
CEO and President, IBM

Be part of a **network** that does **not only** sign up to, but **collaborates** on **Cybersecurity!**

Let us be your
trusted partners
for **cybersecurity**
and **digitalization**

Together we will
improve our
technology, people
and **processes**

Follow
our principles
making the digital
world more secure

And we bring them to life:

Principle 1 — Ownership of cyber and IT security

IBM's approach to ownership
Our **cybersecurity organization**

Our Vision

A **trusted partner** in the digital world, providing industry leading cybersecurity for IBM and our clients

Our Holistic approach

Our Secure Infrastructure



Our Secure Offerings



Our cyber services and solutions



01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – “It is everyone’s task”

And we bring them to life:

Principle 6 — Education

IBM examples of best practices in this principle:

- Veterans cyber training program
- Mandatory cyber training for all employees
- Mobile cyber range for almost real life scenarios for executive training

06 Education

Include dedicated cybersecurity courses in school curricula – As degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future

And we bring them to life :

Principle 2 — Responsibility throughout the digital supply chain

IBM examples of supply chain requirements

- Greatest scrutiny for most significant risks
- Data Centric focus of digital supply chain

Concrete implementation with CoT Partners

With our partners, we are defining a list of minimum security requirements for the supply chain, and the mechanisms to support implementation

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards.

And we bring them to life :

Going into more detail

What does
Responsibility
throughout the digital
supply chain mean?

02 Responsibility throughout the digital supply chain

- Establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements.
- Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards in areas such as:
 - **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
 - **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
 - **Continuous protection:** Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

We have taken the first tangible steps towards increasing trust in Cybersecurity

First result around Principle 2 – Responsibility throughout the digital supply chain


We defined Baseline Cybersecurity Supply Chain Requirements¹⁾

Goal: Make our products and services more secure and introduce a **Cybersecurity standard** for **ourselves** and **our suppliers** by committing to 17 baseline requirements¹⁾

An aligned CoT view on Baseline Cybersecurity Supply Chain Requirements¹⁾ along the digital supply chain

Category	Baseline Cybersecurity Supply Chain Requirements ¹⁾
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data. Data shall be protected from unauthorized access throughout the data lifecycle. The design of products and services shall incorporate security as well as privacy where applicable.
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/segmentation, operational security, physical security, vendor management). Guidelines on secure configuration, operation and usage of products or services shall be available to customers.
Incident Response	Policies and procedures shall be implemented so as not to consent to include back doors, malware and malicious code in products and services. For confirmed incidents, timely security incident response for products and services shall be provided to customers.
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place.
Access, Intervention, Transfer, & Separation	Encryption and key management mechanisms shall be available to protect data. Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced.
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed. Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments. Robust business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption.
Support	A process shall be in place to ensure that products and services are authentic and identifiable. The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available.
Training	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Consulting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support. A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness).

1) For next generation products and solutions.
Source: Charter of Trust – Task force "Baseline Cybersecurity Supply Chain Requirements"¹⁾



Next steps – agree risk based approach, mapping to standards and verification

- Detail baseline requirements to ensure **clear understanding** in the implementation process
- Map baseline requirements to **existing international and regional standards and certification schemes²⁾**
- Categorise **baseline requirements for suppliers** according to different **levels of criticality³⁾**
- **Agree implementation paths** for and next generation products and solutions
- Develop **verification mechanisms** to achieve compliance with baseline requirements – from self declaration to third party certification

1) For next generation products and solutions; 2) For example: ISO 27001, ISO 20243, SOC2, IEC 62443;

3) To be defined by CoT partners (e.g., low – medium – high)

Source: Charter of Trust – Task force "Baseline Cybersecurity Supply Chain Requirements¹⁾"

Aligned CoT view on Baseline Cybersecurity Supply Chain Requirements¹⁾ along the digital supply chain

Category	Baseline Cybersecurity Supply Chain Requirements ¹⁾
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data
	Data shall be protected from unauthorized access throughout the data lifecycle
	The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/ segmentation, operational security, physical security, vendor management)
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services.
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer, & Separation	Encryption and key management mechanisms shall be available, where relevant, to protect data
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable
	A process shall be in place to ensure that products and services are authentic and identifiable
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)

1) For next generation products and solutions

Source: Charter of Trust – Task force "Baseline Cybersecurity Supply Chain Requirements¹⁾"