
jitsun
Truth In Things

Things are only secure until they are not.

How can we “Be Secure”?


IMPROVED
INVIOLABLE
LOCK

Things are only secure until they are not

The Internet of Things

The Internet of Things

Things are only secure until they are not

Energy & Utilities

Transportation

Buildings & Infrastructure

Things are only secure until they are not

Healthcare

Finance & Insurance

Platforms & Digital Services

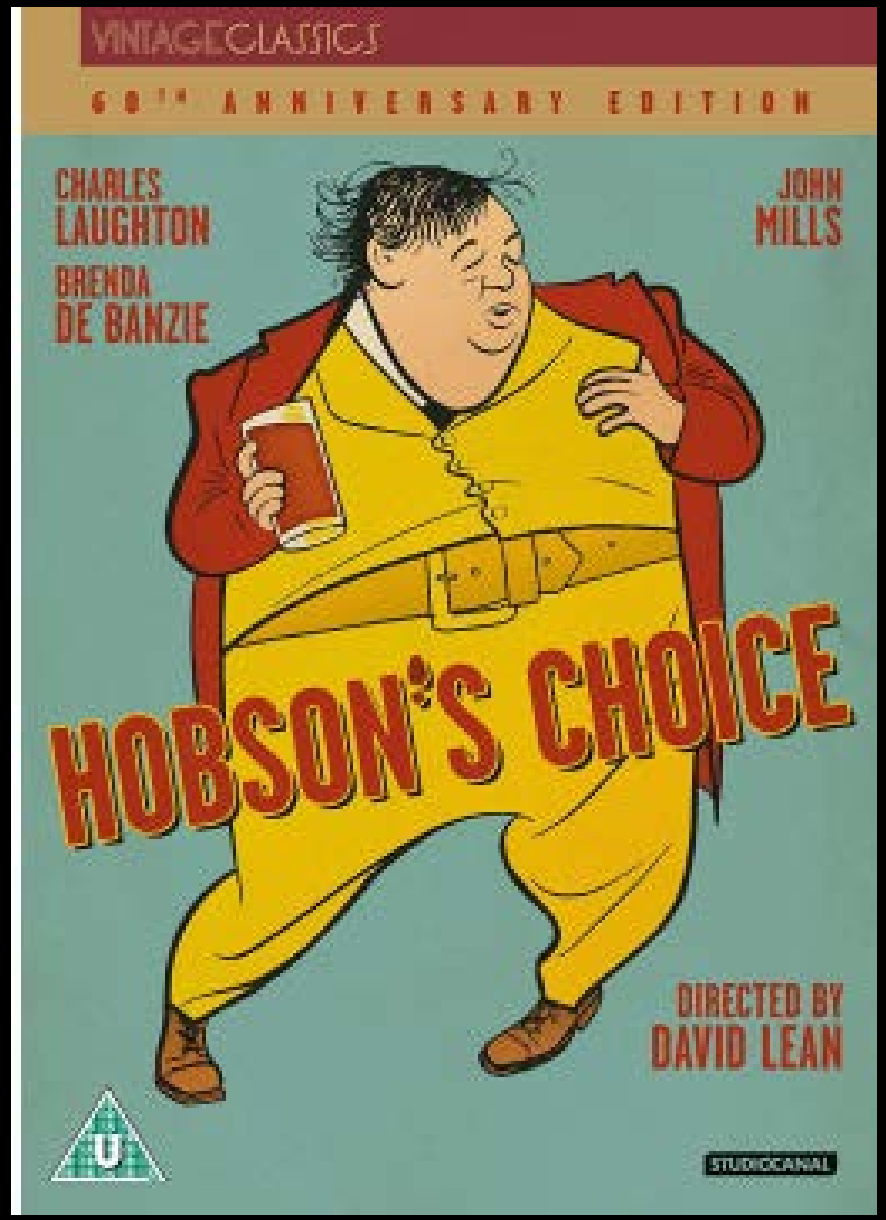
Vulnerability disclosure

“Vulnerability disclosure is an increasingly important topic, especially for providers of Internet-of-Things (IoT) products and solutions. To avoid unnecessary risk to both the providers and users of these offerings when security issues are found by external parties, providers should set expectations of a clear process for responding to reports of such issues and for managing the public disclosure of information regarding them.”

Firmware Updates

“Manufacturers of safety-critical system components should investigate (and be prepared to implement) the types of “IT-like” capabilities users will come to expect, such as firmware updates via the network of their OT systems, while still ensuring safety.”

https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf
https://iotsecurityfoundation.org/wp-content/uploads/2017/01/Vulnerability-Disclosure.pdf



SECURE
or
COMPLIANT

It's your CHOICE

9 May 2018

Network Information Systems Directive 28 EU Member States Adoption

Enact Directive into National Law
Establish Competent Authorities (Regulators)
Determine Operators of Essential Services
Reporting Obligations
Create Sanctions Regimes

Energy supply – Oil & Gas, Electricity
Transportation – Rail, Road, Sea, Air
Telecommunications – Mobile, broadband
Healthcare – Hospitals, medical equipment
Buildings & Infrastructure – Smart city, HVAC, Lighting
Digital Service Providers – Platforms & Markets

Implementation Phase → Enforcement

Mind the Gap!

Technology Suppliers ← → Operators of Essential Services

RISKS

Penalties for non-compliance
- Corporate fines (UK £17m)
- Individual director fines
- Imprisonment (Croatia)

Notifications within 72 hours
Double jeopardy with GDPR

Past | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Future

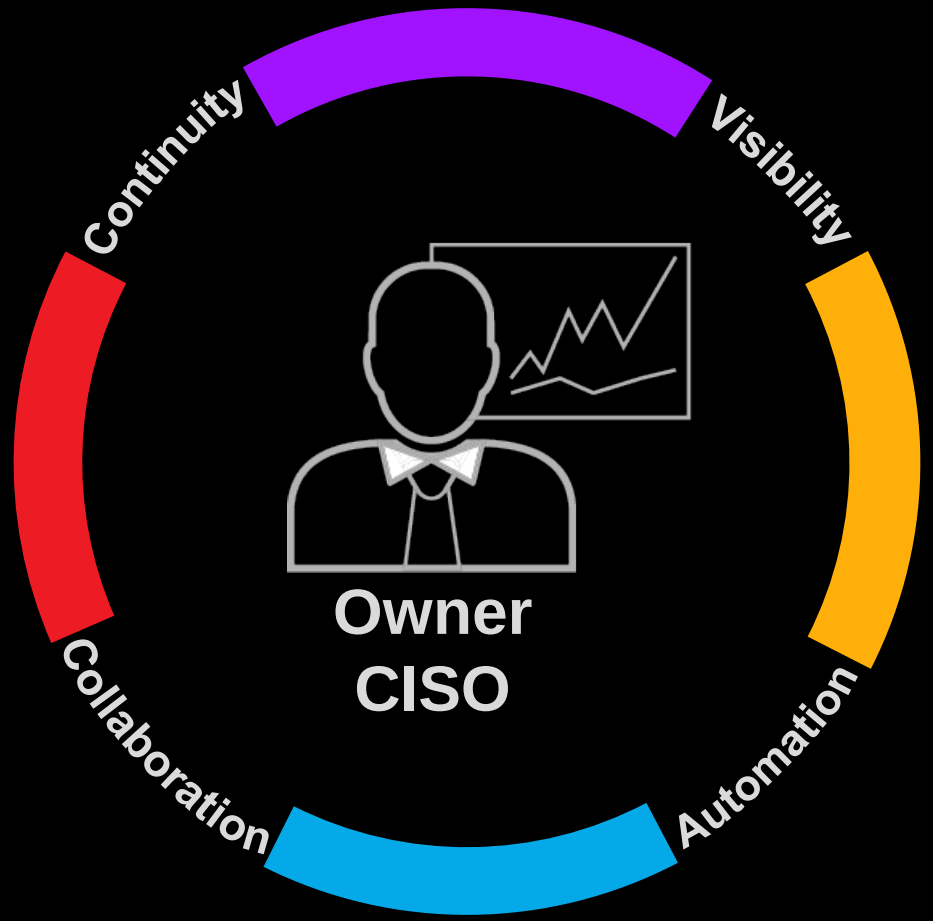
2019 | 2020

Operational Pressures

- ✘ Invisible supply chain risks
- ✘ Proving NISD compliance
- ✘ Constrained budgets

Operational Pressures

- ✘ Invisible supply chain risks
- ✘ Proving NISD compliance
- ✘ Constrained budgets



Centre for Connected and Autonomous Vehicles

Centre for the Protection of National Infrastructure

Department for Transport

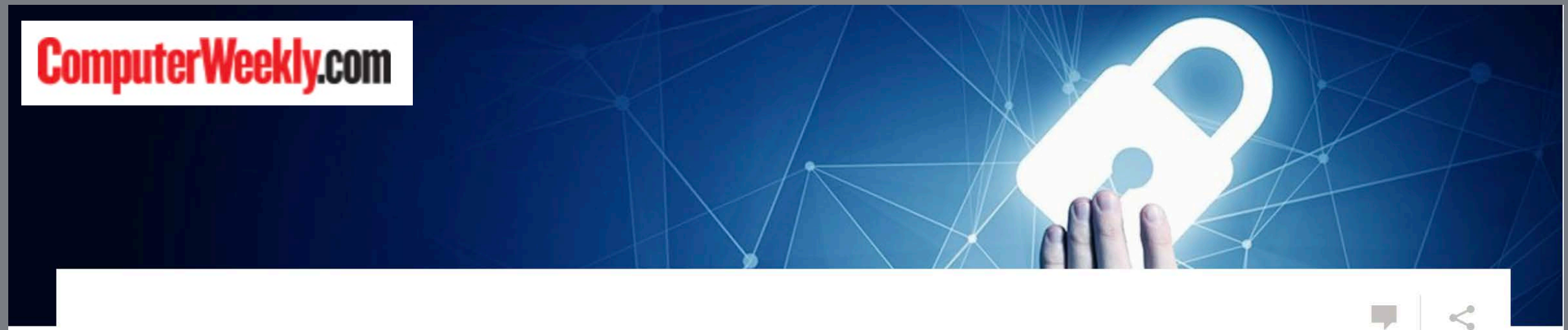
Guidance

The key principles of vehicle cyber security for connected and automated vehicles

Published 6 August 2017

Principle 1 - organisational security is owned, governed and promoted at board level
Principle 2 - security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain
Principle 3 - organisations need product aftercare and incident response to ensure systems are secure over their lifetime
Principle 4 - all organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system
Principle 5 - systems are designed using a defence-in-depth approach
Principle 6 - the security of all software is managed throughout its lifetime
Principle 7 - the storage and transmission of data is secure and can be controlled
Principle 8 - the system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail

ComputerWeekly.com



Cyber security is a team sport, says NCSC

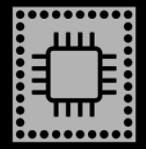
The UK's national cyber security agency aims to help organisations understand the need to act collaboratively and collectively against the cyber threat, urging them to raise the bar

By **Warwick Ashford,** Senior analyst

Published: 07 Mar 2018 10:51

UK organisations can learn from sport in how they prepare for and execute cyber defence programmes, according to the National Cyber Security Centre (NCSC).

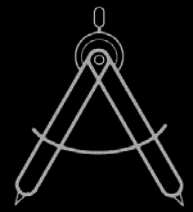
How do we move fast and fix Things?



Chip Maker

Thing Maker

Patch



Integrator

Test

Owner

Approve

System Operator

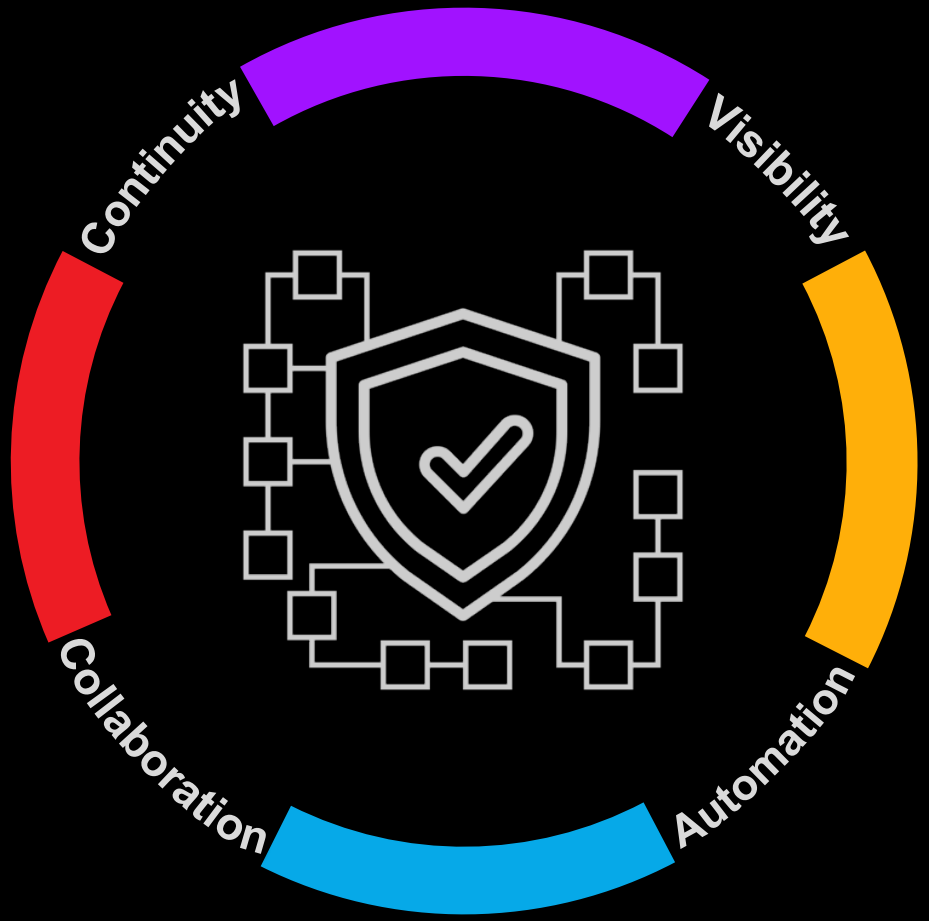
Schedule

Auditor

Monitor

Third Party

Distributed ledgers have the attributes



- **Visibility**
  all stakeholders see the same state and transaction history
- **Collaboration**
  all stakeholders reach consensus on transactions
- **Continuity**
  Distributed records mean no single actor can corrupt records or take down service
- **Automation**
  Distributed apps act on events

Plugging the gap

How Distributed Ledgers help operators Be Secure

A permanent record of when who did what to a Thing…

when

timestamped chain of transactions

who

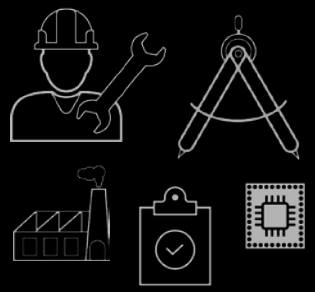
did what

to what

action : report vulnerability, safety inspection, update parameters, install software, move/transfer, factory restart …

thing identity

transaction structure

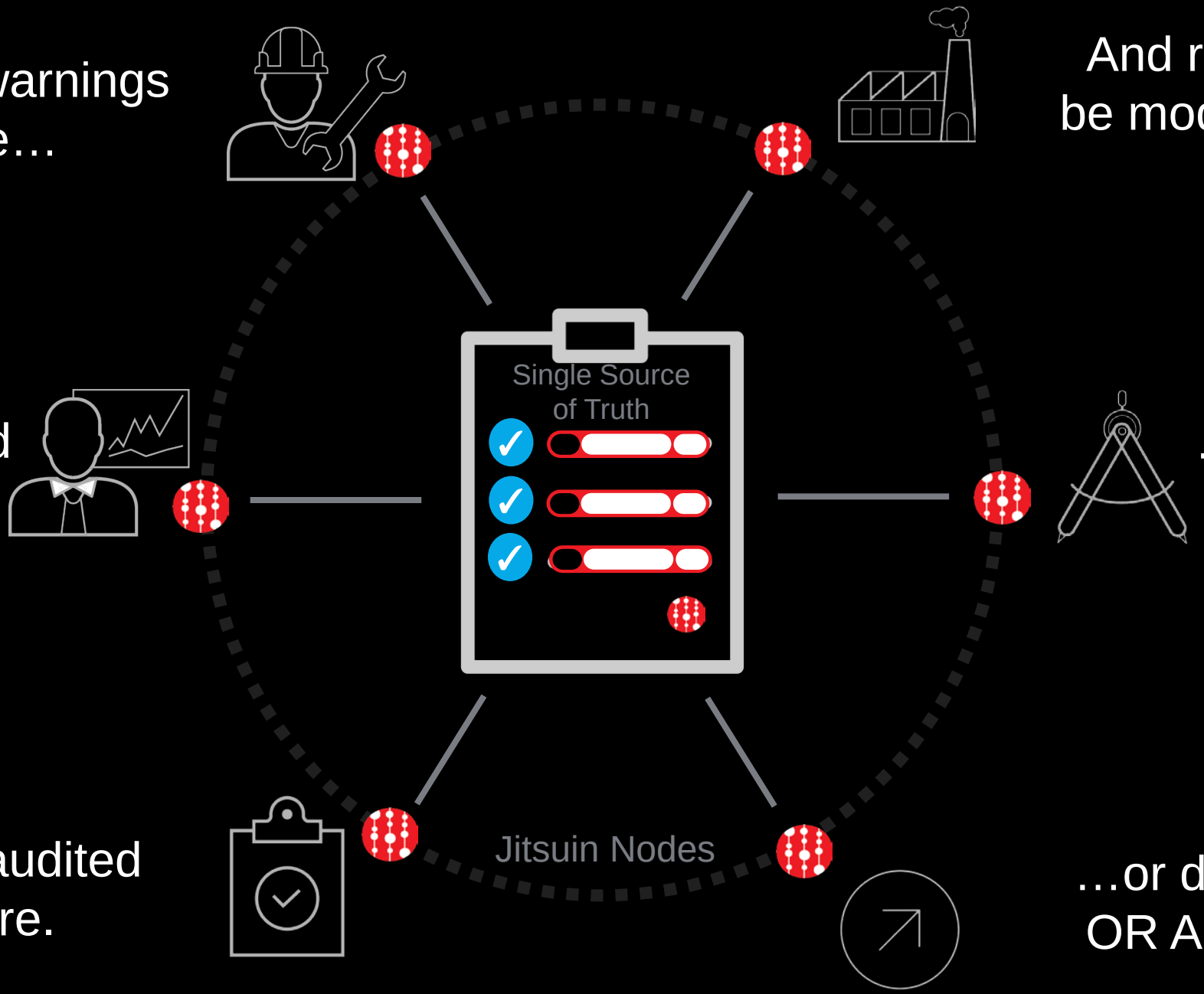


…that can deliver actionable intelligence.

Actions and warnings recorded here…

…are safely replicated and actionable here…

…and can be audited and verified here.



And records can't be modified here...

…or falsified here…

…or deleted here. OR ANYWHERE.

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

NIST CYBERSECURITY FRAMEWORK

jitsuin

WHITE PAPER

Achieving Continual Compliance to NISD

jitsuin.com info@jitsuin.com

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

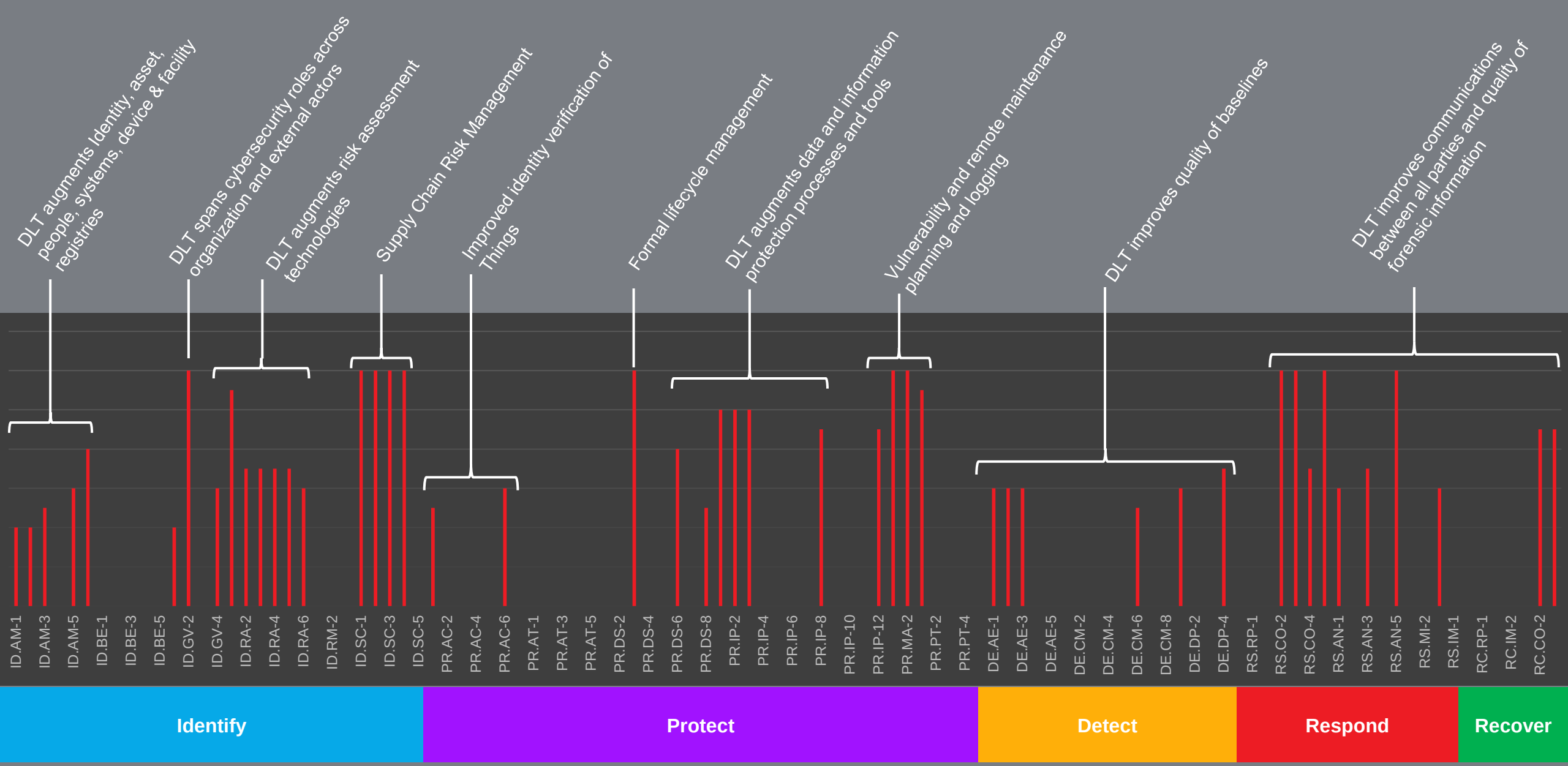
NIST
CYBERSECURITY FRAMEWORK

jitsuin

WHITE PAPER

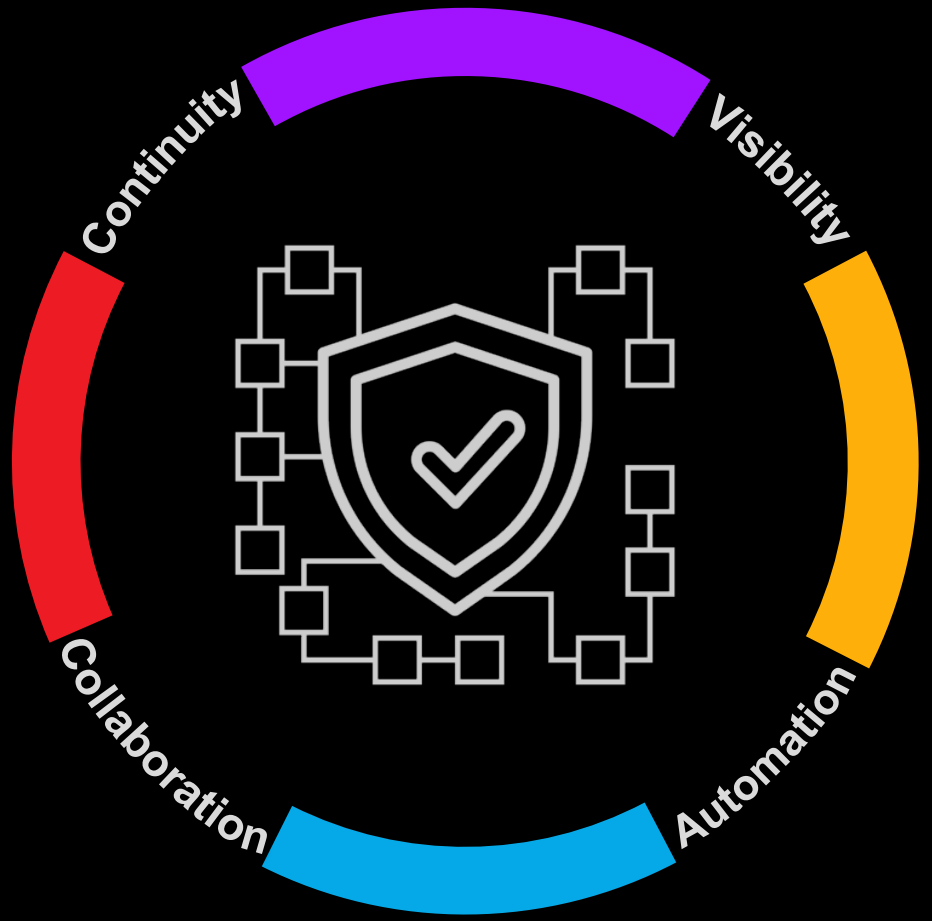
Achieving Continual Compliance to NISD

jitsuin.com info@jitsuin.com



NIST CSF v1.1 scored on DLT Attributes of Collaboration, Visibility, Continuity and Automation

Shared Ledger System



Alternatives

- ✘ Paper Records
- ✘ Shared Database
- ✘ Trusted Third Party

Take-aways

- NISD, CSF, and many other regulations are coming
- The scale of the challenge and the pace of change is too great for traditional approaches
- The best way to BE SECURE is to actively manage risks in the Continuous Digital Supply Chain
- It’s a TEAM SPORT

- Download the whitepaper from https://Jitsuin.com

jitsun

Truth In Things

Thank you

Jon Geater
Co-Founder & CTO