GROUP

CYBERSECURITY 4 PLANTS
THE CERTIFICATION EFFORT

www.bitron.net

ABSTRACT

As of today the wargames are played in the cyberspace: the attacker (an individual or, more often, an organization) applies his effort to drill the defense countermeasures of the defender.
To have success the attacker has to win just once, the defender must win always.
In the automotive industry the fear to be drilled is continuously increasing at OEM side.
The component/system suppliers must therefore adhere to very high demanding cybersecurity standards to comply with the requested levels of security.
Many Security Information Management Systems (ISMS) standards and rules are then born (European + German, American, Japanese), like ISO27001, ISO21434, TISAX, IEC62443, R155 & 156. And don' t forget the GDPR.
Though an ISMS can be "corporate", how big is the effort, in time and cost, to reach such variety of certifications for many plants?
And, this is the question: "is one -or many- certification enough to win the (war)game ?"
Stay tuned to discover...

THE INFORMATION SECURITY: THE COMMUNICATION EVOLUTION

THE AUTOMOTIVE OEM's REQUIREMENTS

THE CYBERSECURITY IN THE AUTOMOTIVE AND INDUSTRIAL WORLDS

THE TISAX ASSESSMENT

THE INTEGRATION BETWEEN ISO27001 & TISAX

THE ISMS: INTEGRATED OR STAND ALONE ?

THE CERTIFICATION PATH FLOW-CHART

THE INTEGRATED MANAGEMENT SYSTEM APPROACH / THE DOCUMENTATION

THE PHYSICAL DEFENSE SYSTEM

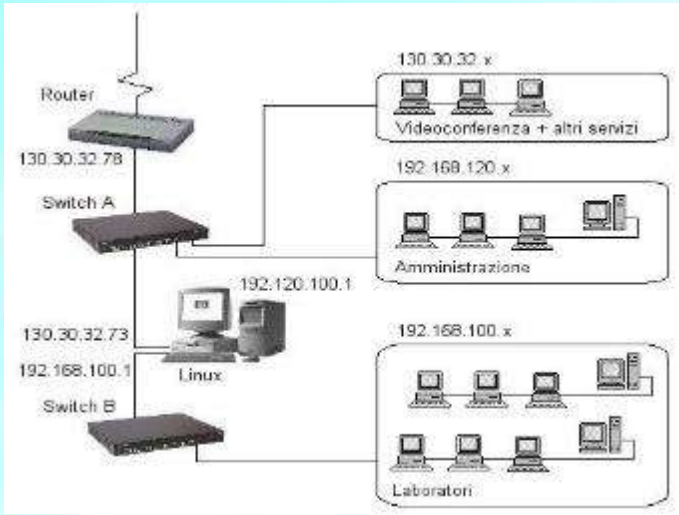
THE PLANT vs VULNERABILITY ASSESSMENTS & PENETRATION TEST

THE CONTINUOUS IMPROVEMENT ON ISO27001 (& TISAX)

THE TISAX PROTOTYPES MANAGAMENT REQUIREMENTS

THE NEEDS OF AN INFORMATION SECURITY DEPARTMENT

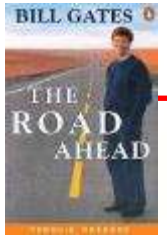
INFORMATION SECURITY: THE COMMUNICATION EVOLUTION



GUTENBERG
mobile characters

THE ROSETTA STONE

5000A.C. → 1450 → 1980 MILITARY NETWORKS (ARPANET)



1994 INTERNET

WWW

2020

SMART-PHONE-CAR-TV…

THE TARGET FOR HACKERS WIDENS

5000Ac — THE PRIVACY BORN IN USA IN 19TH CENTURY: «Let me be alone»

1450 1980 1990 2020

INFORMATION SECURITY: THE COMMUNICATION EVOLUTION (2)

NASA COMPUTER FOR APOLLO 11

1969

ITS SOFTWARE «TOWER»

150 millions of Apollo 11 mainframes in one iPhone 7

1980

2021

The computing power of the whole Europe in the 80ies stays in one today's smartphone

THE AUTOMOTIVE OEM's REQUIREMENTS

- **THE AUTOMOTIVE OEM's ARE REQUESTING THEIR SUPPLIERS TO GUARANTEE THE INFORMATION SECURITY FOR THE WHOLE PRODUCT LIFECYCLE.**

- **A WIDE VARIETY OF RULES HAS BEEN THEN PREPARED, BY SEVERAL AUTHORITIES LIKE ISO, SAE, IEC, TISAX, TO *INSTRUCT* THE COMPANIES TO ADOPT AN INFORMATION SECURITY MANAGEMENT SYSTEM**

- **BEING CERTIFIED WITH RESPECT TO SOME OF THOSE RULES HAS BECOME MANDATORY IN BUSINESS RELATIONSHIPS. SOME OEM's REQUIRE THE SUPPLIER TO BE CERTIFIED EVEN TO RECEIVE A NEW RFQ.**

THE CYBERSECURITY IN THE AUTOMOTIVE AND INDUSTRIAL WORLDS

TISAX®
RESULT AVAILABLE

Information Security Management ISO 27001 Certified

EU 2016/679 GDPR
«PRIVACY LAW»

ATF®

- ISO 21434
- SAE J3061
- ISO 26262
- ISO 33001

EMBEDDED WORLD

BITRON
GROUP

- IEC 62443-2-1
- IEC 62443-4-1
- IEC 62443-4-2

E 1 …

UNECE GRVA-09-16

R155

R156

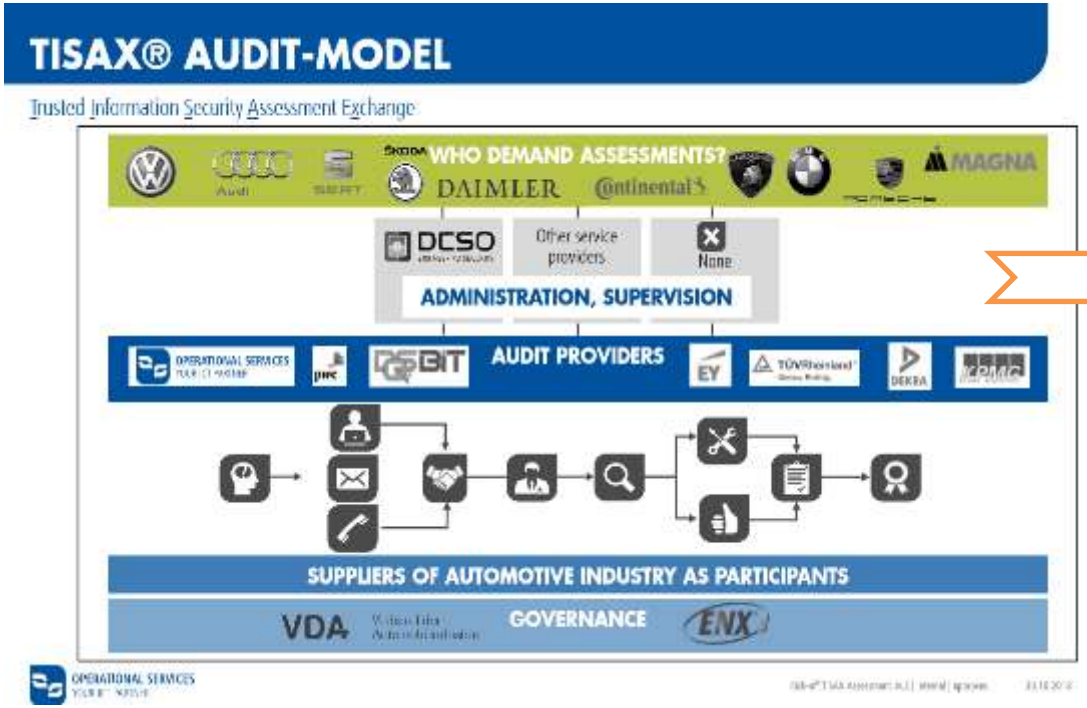
…COMMON CRITERIA…15408

THE TISAX ASSESSMENT

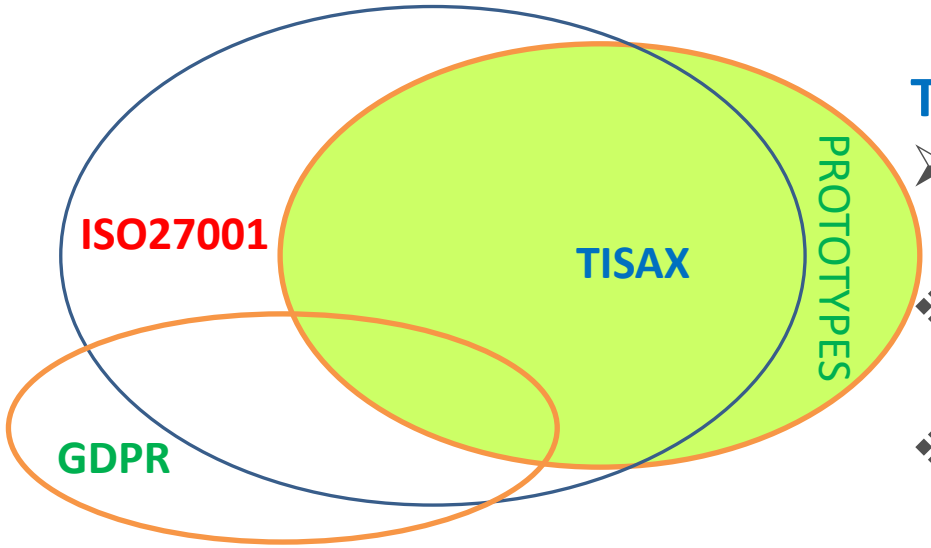
TISAX STANDS FOR: Trusted Information Security Assessment eXchange AND REPRESENTS A GERMAN CONSORTIUM OF AUTOMOTIVE OEM's.

BASED UPON THE VDA-ISA CHECKLIST; THE ASSESSMENT RESULTS ARE THEN SHARED ON THE ENX PLATFORM.

THE RESULT GIVES A «MATURITY LEVEL»: ONCE POSITIVELY PASSED THE ASSESSMENT, THE COMPANY RECEIVES A LABEL OF COMPLIANCE, VALID FOR THREE YEARS



THE INTEGRATION BETWEEN ISO27001 & TISAX



TISAX® combines:

- The rules on Information Security (ISA) of Verband der Automobilindustrie (VDA)
- The Annex A (Technical Controls) of ISO / IEC 27001
- Some privacy requirements (GDPR).

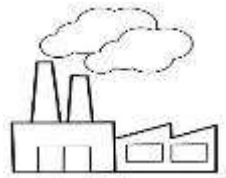
TISAX® and ISO27001 are very similar: the TISAX maturity level concept is compatible with the ISO27001 certification.

Both systems contain requirements that are plant specific (i.e. physical and environmental security controls), therefore although the certification can be «corporate», anyway the certificate is issued for every single plant (specifically for TISAX prototypes requirements).

THE ISMS: INTEGRATED OR STAND ALONE ?

AS OF TODAY, AN ORGANIZATION CANNOT BE FOCUSED ONLY ON A SINGLE (QUALITY) MANAGEMENT SYSTEM, BUT IT SHALL CONSIDER MULTIPLE SYSTEMS, INTEGRATED TOGETHER, SUCH AS:

- **QUALITY - IATF 16949 & ISO 9001**
- **ENVIRONMENT - ISO 14001**
- **HEALTH & SAFETY - ISO 45001**
- **INFORMATION SECURITY - ISO 27001 (and/or TISAX and/or ISO62443 and/or….)**



…..AND DON'T FORGET THE:

- **SUSTAINABILITY (ISO16001)**
- **General Data Protection Regulation - GDPR (EU 679/2016)**

SINCE MAY 2018 HAS BECOME OPERATIONAL THE EUROPEAN LAW ON PERSONAL DATA HANDLING: EU 679/16 (GDPR)

GENERAL DATA PROTECTION REGULATION - GDPR

THE FLOW TO IMPLEMENT AN ISMS AND TO REACH THE CERTIFICATION IS:

1. **PRE-ASSESSMENT : TO BE DONE ON EACH PLANT, TO VERIFY THE STATUS OF THE INFORMATION MANAGEMENT (AND THE LOCAL IT FUNCTION) AGAINST THE «ANNEX A» CONTROLS**

2. **ASSET INVENTORY: THE LIST OF ASSETS (HW, SW, HR, LOCATIONS) THAT ARE INVOLVED IN THE INFORMATION MANAGEMENT AND THAT CAN CAUSE A LOSS OF Confidentiality/Integrity/Availability (CIA) OF INFORMATION**

3. **POLICY: THE VERY FIRST DOCUMENT THAT STATES THE ACCOUNTABILITY OF THE COMPANY (i.e. TOP MANAGEMENT) AND DECLARES THE STRATEGIES TO BE APPLIED IN THE COMPANY'S ISMS.**

4. **RISK MANAGEMENT: BASED ON THE ASSET INVENTORY AND APPLYING THE ISO27005 METHODOLOGY, THE ANALYSIS OF THE RISKS ASSOCIATED TO THE ASSETS, THEIR MITIGATION COUNTERMEASURES, THE ACCEPTABILITY METRICS.**

THE CERTIFICATION PATH FLOW-CHART (2)

….THE FLOW TO IMPLEMENT AN ISMS AND REACH THE CERTIFICATION IS:

5. **PROCEDURES-GUIDELINES: THE DOCUMENTS, WHICH DESCRIBE HOW TO MITIGATE THE IDENTIFIED RISKS, SHALL BE PREPARED**

6. **MEASUREMENT: THE GUIDELINES DEPLOYMENT IN THE PLANTS, AND THE INITIAL EFFICACY MEASUREMENT: EVIDENCES, KPI's, PERSONNEL TRAINING, INTERNAL AUDIT, MANAGEMENT REVIEW. AFTER 2/3 MONTHS AN ITERATION OF MEASUREMENT HAS TO BE DONE.**

7. **PHASE 1 ASSESSMENT: THE ISMS BEING A PART OF THE (INTEGRATED) MANAGEMENT SYSTEM OF THE COMPANY IS CHECKED: POLICIES, GUIDELINES, RISK MANAGEMENT, S.O.A., B.I.A., ACCOUNTABILITY, KPI'S, INCIDENT MANAGEMENT, DISASTER RECOVERY PLAN, ANNEX A CONTROLS APPLICATION AND VERIFICATION.**

8. **PHASE 2 ASSESSMENT: AFTER A VARIABLE TIME (MIN 2 WEEKS, MAX 6 MONTHS) A SERIES OF INTERVIEWS IS DONE TO THE PROCESS OWNERS BASED ON THE ASSET INVENTORY AND HOW THEY MANAGE THE ASSOCIATED RISKS. THE EFFICACY RECORDS OF THE IMPLEMENTATION COMPOSE THE REPORT OF CERTIFICATION**

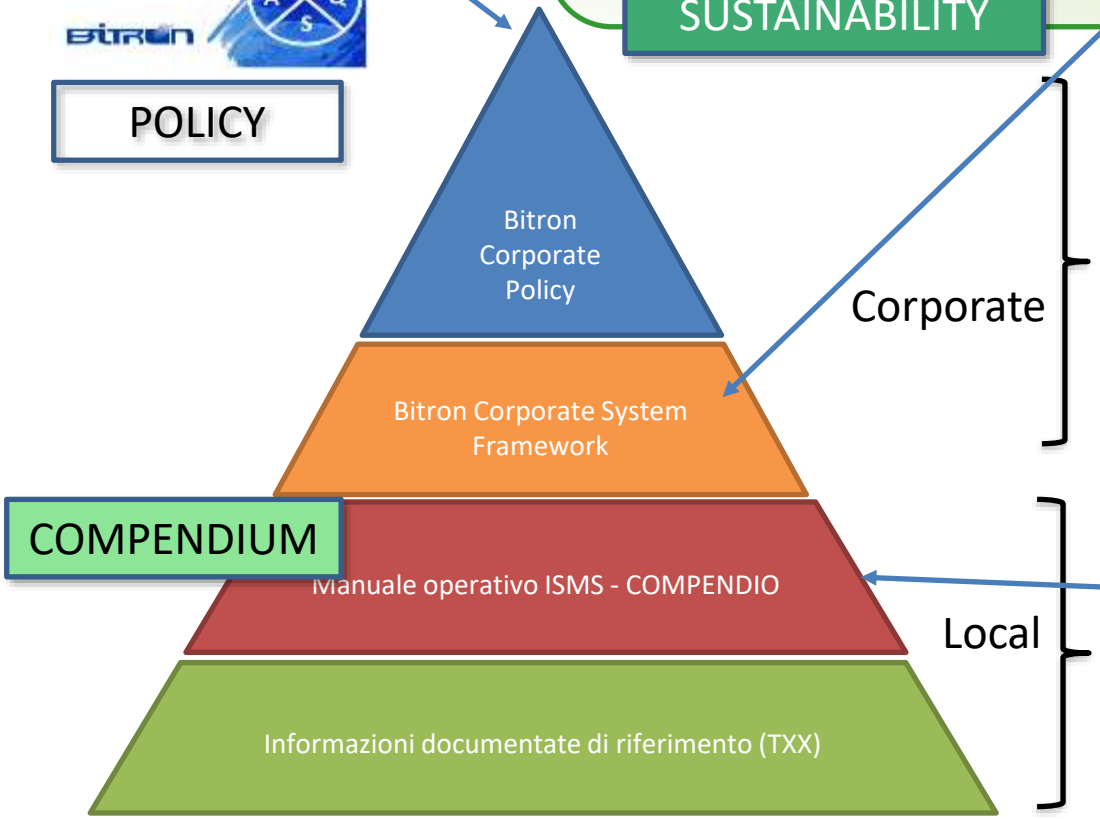
AN INTEGRATED MANAGEMENT SYSTEM DOCUMENTATION APPROACH

Framework comune ai sistemi di gestione

- Sistema di Gestione della Qualità (QA)
- Sistema di Gestione Salute e Sicurezza sul Lavoro (SSL)
- Sistema di Gestione Ambientale (ENV)
- Sistema di Gestione Sicurezza delle Informazioni (ISMS-GDPR)

SUSTAINABILITY

POLICY



COMPENDIUM

THE PHYSICAL DEFENSE SYSTEM (1)

CYBERSECURITY DEALS ALSO WITH THE PHYSICAL PROTECTION MEASURES:

FENCES, OBSCURED WINDOWS, ELECTRONICALLY CONTROLLED GATES, CAMERAS, MANNED SURVEILLANCE SYSTEM, DOORS WITH AUTOMATIC CLOSURE SPRINGS, ANTITHEFT ALARMS, SEPARATED IN/OUT PATHS FOR TRUCKS, METALLIC CUPBOARDS, STRONGBOXES…*NO LIMITS TO AUDITORS' FANTASY*…

THE PHYSICAL DEFENSE SYSTEM (2)

THE INTERNAL LAYOUT MAPS SHALL INDICATE WHICH AREAS ARE MOST CRITICAL: A CRITICALITY LEVEL SHALL BE ASSIGNED AND WHICH RISK MITIGATION MEASURES HAVE BEEN TAKEN INTO ACCOUNT SHALL BE DESCRIBED (AND MAINTAINED) AS WELL.

ANY PLANT SHALL SUSTAIN YEARLY A VAPT ATTACK (AT LEAST) ON:

- MAILS ACCESS
- CREDENTIALS ACCESS
- FILE SERVER ACCESS
- BACKUPS ACCESS
- ORGANIZATION 'S SERVERS
- ERP SYSTEM ACCESS
- PLM SYSTEM ACCESS
- PHYSICAL ACCESS

THE CONTINUOUS IMPROVEMENT IN ISO27001 (& TISAX)

ISO27001:

- A COMPLETE CERTIFICATION ASSESSMENT SHALL BE HELD ON ALL THE FUNCTIONS OF A PLANT EVERY THREE YEARS (Y0)
  - A VERIFICATION ASSESSMENT ON ONE HALF OF THE FUNCTIONS AFTER ONE YEAR (Y1)
    - A VERIFICATION ASSESSMENT ON THE SECOND HALF OF THE FUNCTIONS ON THE SECOND YEAR (Y2)

Y0 Y1 Y2 Y0 Y1 Y2 Y0 ……..

TISAX® :

A COMPLETE CERTIFICATION ASSESSMENT ON ALL THE FUNCTIONS OF A PLANT + **PROTOTYPES MANAGEMENT** EVERY THREE YEARS (Y0)

Y0 Y0 Y0 ……..

In the Corporate approach the Headquarter holds a complete assessment (3.5 days), while the other plants hold a one day assessment, mainly to assess the application of the gudelines and the compliance of physical aspects and the prototypes management.

THE TISAX PROTOTYPES MANAGAMENT REQUIREMENTS

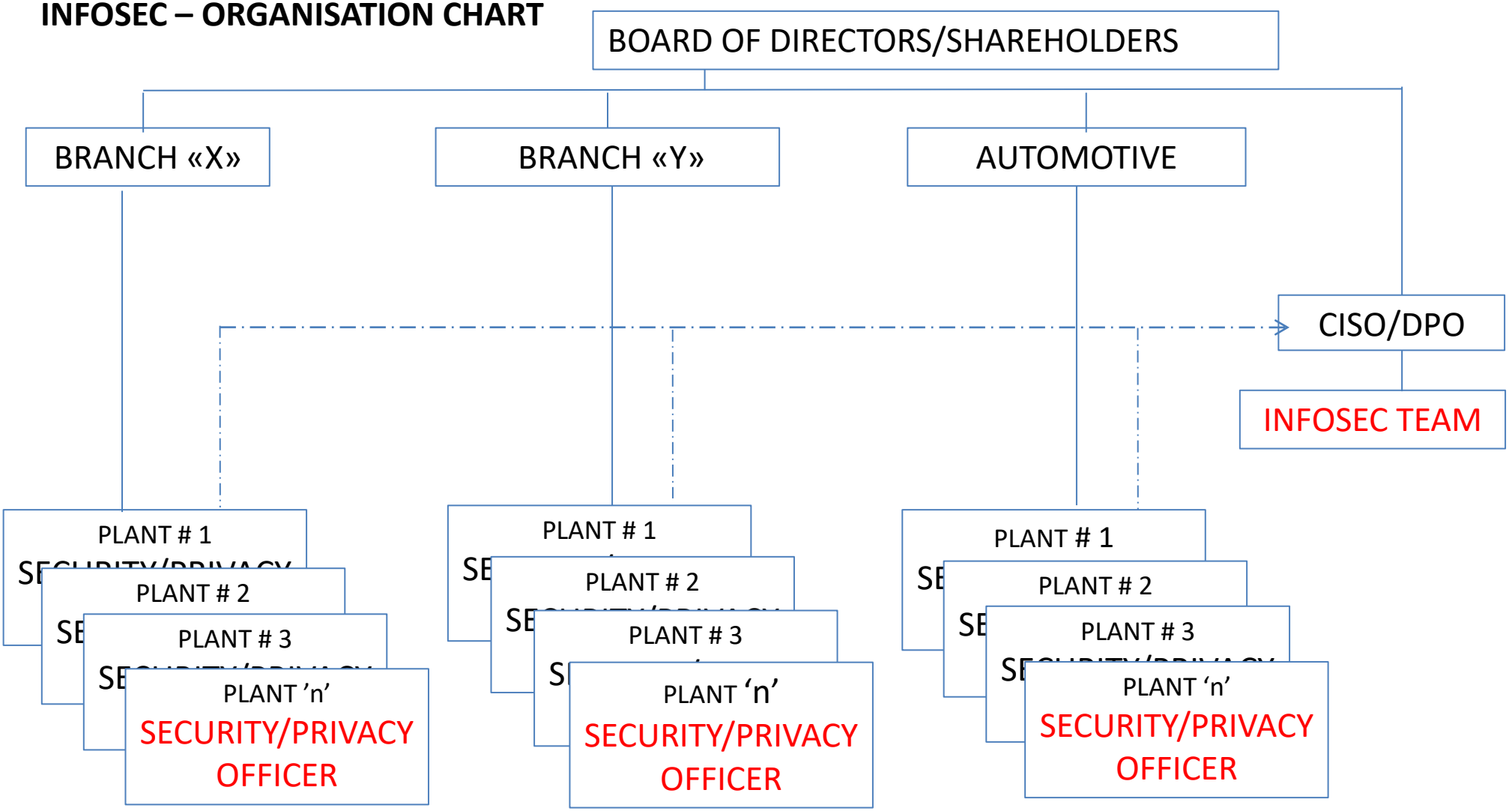
ACCORDING TO VDA-ISA A PROTOTYPE IS «**EVERYTHING THAT IS NOT YET ON THE MARKET**»

TO COMPLY WITH TISAX PROTOTYPES MANAGEMENT REQUIREMENTS YOU MUST:

- **HAVE A GUIDELINE/PROCEDURE CONFORM TO : VDA_Minimum_Requirements_for_Prototype_Protection (available on the web)**
- **ORGANIZE AN AREA WHERE THE PROTOTYPES ARE ASSEMBLED, TESTED, STORED, DISPATCHED. THIS AREA MUST HAVE:**
  - **DOORS WITH AUTOMATIC CLOSURE (i.e. springs)**
  - **ELECTRONICALLY CONTROLLED ACCESS (i.e. badge)**
  - **ALARM SYSTEM (certified DIN EN 50131, or conform to VDS, or similar rules)**
  - **OBSCURED WINDOWS (i.e. not completely transparent – but remember the ISO45001)**
  - **METAL CUPBOARDS FOR STORAGE (with keys assigned only to authorized persons)**
- **ONLY TRAINED AND AUTHORIZED PERSONNEL CAN HAVE ACCESS TO THAT AREA**
- **MASK OFF PARTS IN CASE OF VISIT (CUSTOMER «A» MUST NOT SEE PROTOTYPES OF «B»)**
- **PHOTO SHOOTING FORBIDDEN (ALSO FOR THE CUSTOMER)**
- **MASK OFF PROTOTYPES WHEN MOVING THEM BETWEEN PLANT'S AREAS (i.e. box them over)**

THE NEED OF A DEDICATED INFOrmationSECurity DEPARTMENT

INFOSEC – ORGANISATION CHART



CISO **C**hief **I**nformation **S**ecurity **O**fficer

DPO **D**ata **P**rotection **O**fficer -- **SO** **S**ecurity **O**fficer -- **PO** **P**rivacy **O**fficer

The end of the story….

THE INITIAL QUESTION WAS: DOES THAT ALL GRANT THE INFORMATION SECURITY ?

SURE….NOT !

SO, WHY DO WE DO ALL THIS ?

NOT ONLY BECAUSE THE OEM's REQUIRE IT, OF COURSE, BUT ALSO :

- **BECAUSE THE PATH TO GET A CERTIFICATION REQUIRES THAT ALL THE PEOPLE IN A COMPANY SHALL RAISE THEIR ACCOUNTABILITY IN THIS MATTER**
- **BECAUSE THE COMPANY MUST TAKE INTO ACCOUNT ADEQUATE INVESTMENTS (BUDGET FOR HW, SW & PEOPLE)**
- **BECAUSE *«THE WEAK RING IN A CHAIN»* IS ALWAYS THE HUMAN FACTOR, AND THE BEST SOLUTION FOR THIS, IS TO INCREASE THE KNOWLEDGE ON «CYBER RISKS» BY INVOLVING ALL THE EMPLOYEES, THROUGH A STRONG TRAINING AND A STRONG COMMITTMENT OF THE BOARD.**
- **BECAUSE THE NEXT CHALLENGE IS TO FIGHT AGAINST TRUE CYBERCRIMINAL ORGANIZATIONS, NOT JUST AGAINST A BOY….**

… ooops … not really the end: how much it costs ?

ISO27001 or TISAX:

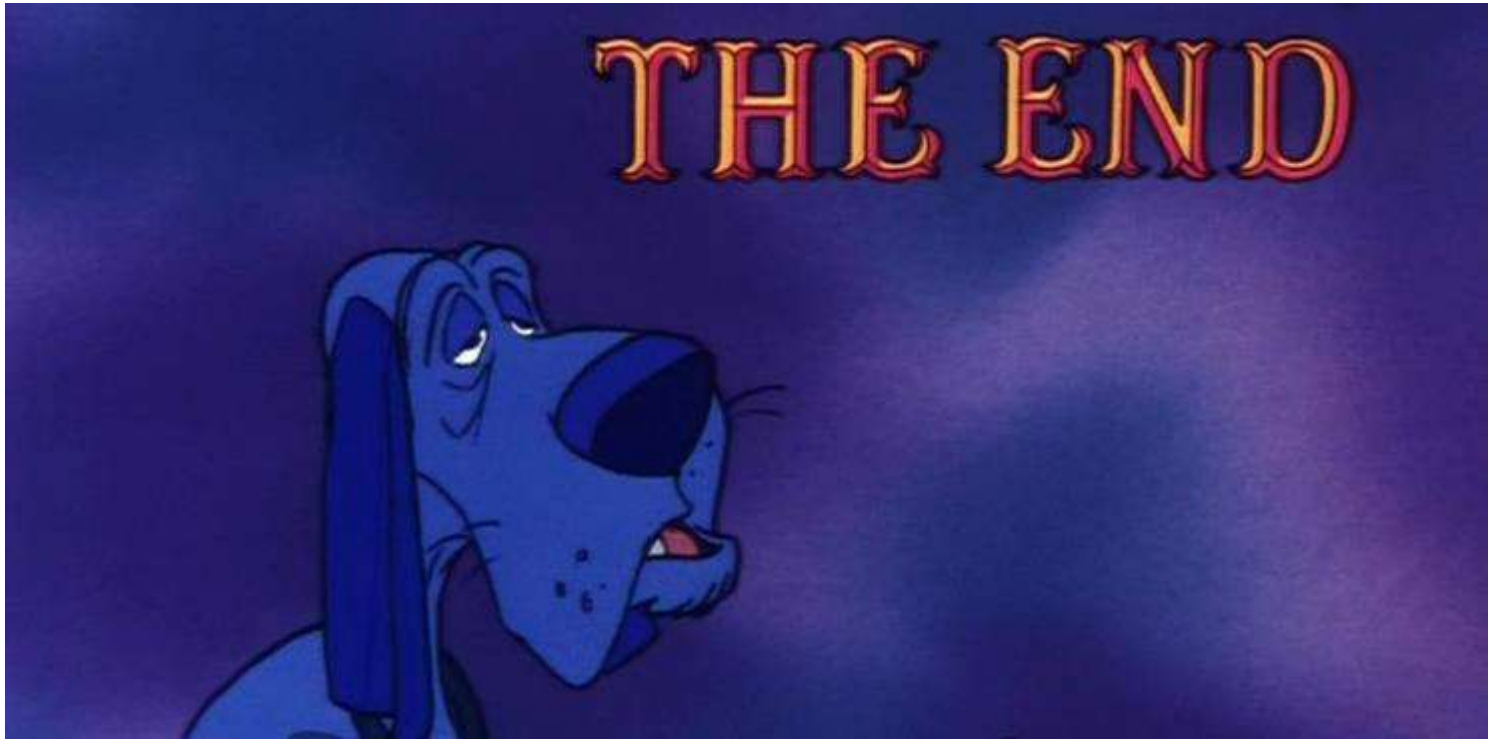
RAW CERTIFICATION COST +/- 10 KEURO x PLANT, PLUS anything of the following whether not yet available:

- **+ LOG MANAGEMENT TOOLS (USERS LOGS)**
- **+ PAM TOOLS (ADMINISTRATORS LOG)**
- **+ AV ON ALL ENDPOINTS**
- **+ ENCRYPTION AND DUAL AUTHENTICATION TOOLS**
- **+ e-LEARNING TOOLS**
- **+ GDPR MANAGEMENT TOOLS**
- **+ PHYSICAL ADD-ON's**
- **+ DATA CENTERS REDUNDANCY AND BUSINESS CONTINUITY FACILITIES**
  - ***>>> C/W DELOCALISED DISASTER RECOVERY SERVICE***
- **+ YEARLY VAPT (POSSIBLY A RED-TEAM)**
- **+ CONSULENCY (FOR THE FIRST APPROACH IS HIGHLY RECOMMENDED)**

IF YOUR BOSSES OR STAKEHOLDERS DON'T WANT TO PAY FOR THAT, TELL THEM THAT THEY SHALL:

- ***BE PREPARED TO RUN OUT OF THE AUTOMOTIVE BUSINESS***
- ***BE PREPARED TO PAY THE RANSOMS***
- ***BE PREPARED TO OTHER AWESOME THINGS…NOT YET KNOWN***

… the true end ….



QUESTIONS ? *ugo.schiara@bitron-ind.com*