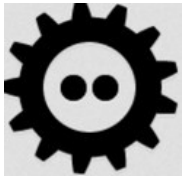
The EU Cybersecurity Act

FOSDEM 2019

Hans de Raad

ULB - Brussels

OpenNovations
by DevHdR



About yours truly

- Hans de Raad
  - ICT / Information (security) Architect / Consultant in:
    - pharmaceutical, healthcare, government,
    - enterprise, education environments
  - Ethical hacker, security tester, teacher / coach
  - Organiser of classical music festivals, classic cars lover, hackerfestivals, amateur wine maker, etc
    - Everyone needs a hobby :-)
    - Former organizer of openSUSE Conference 2015 in The Hague!

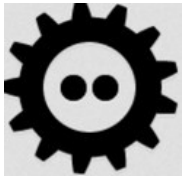
OpenNovations by DevHdR

All the cybers….

OpenNovations
by DevHdR

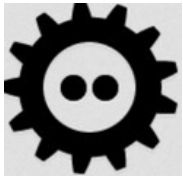
What is “Cyber”?

- Wikipedia:
  - Cyber- is derived from "cybernetic," which comes from the Greek word κυβερνητικός meaning skilled in steering or governing.
  - It is mainly used in the terms cyberspace, cyberlaw, cyberbullying, cybercrime, cyberwarfare, cyberterrorism, cybersex, and cyberdelic among others.
  - Although it is more commonly used to describe policies and politics regarding computer systems and networks (as in the above cases), it is also widely used by many information technology industries.
  - Cyber is now considered as a recent term in the internet era.



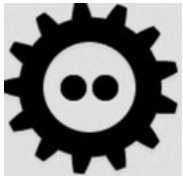
Again, what is “Cyber”?

- Nowadays the dominant term to describe anything spookily internetty/webby/blockchainy/ etc.
  - An example of a term adopted for lack of any other more catchy, relevant and adequate.



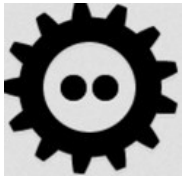
Point of origin

- EU Cybersecurity strategy
  - NIS directive → Cyber security strategy 2013
  - ENISA / ETSI
  - Digital single market
  - GDPR
- US
  - Common criteria / FIPS / etc



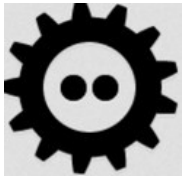
Law always comes last

- But law beats technology
  - In the 1990's US antitrust laws required break-up of large (monopolist) ISPs.
  - Since then technology went too fast to keep up
    - Yet recent (Facebook) hearings in US Senate and EU Parliament indicate the lawmakers are catching up
  - Move from "specified lawmaking" (includes technology) to "conceptualized lawmaking" (outlined principles, requirements and boundaries)



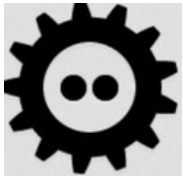
Current cybersecurity approach

- Mostly on national member state level
- Product / incident / disaster prevention oriented
- National Cyber Security Center in NL issues whitepapers on best practices for:
  - Workplace / workstation / ICT infrastructure security
  - Web application security
  - Not: Information security management systems and information governance



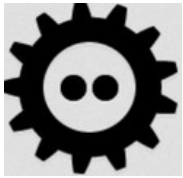
The newly proposed Cyber security regulation

- The proposed Regulation provides for a comprehensive set of measures that build on previous actions and fosters mutually reinforcing specific objectives:
  - Increasing capabilities and preparedness of Member States and businesses;
  - Improving cooperation and coordination across Member States and EU institutions, agencies and bodies;
  - Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises;



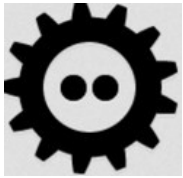
The newly proposed Cyber security regulation

- The proposed Regulation provides for a comprehensive set of measures that build on previous actions and fosters mutually reinforcing specific objectives:
  - Increasing awareness of citizens and businesses on cybersecurity issues;
  - *Increasing the overall transparency of cybersecurity assurance ** of ICT products and services to strengthen trust in the digital single market and in digital innovation;*
  - and
  - Avoiding fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors.



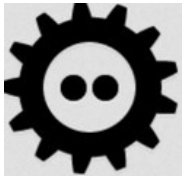
The newly proposed Cyber security regulation

- Increasing the overall transparency of cybersecurity assurance ** of ICT products and services to strengthen trust in the digital single market and in digital innovation;
  - ** Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.



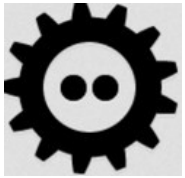
Towards a risk based security strategy

- Security (only) by checklist (ISO27002) is obsolete
  - Just when compliance / QA officers started to use them…
- Blacklisting versus whitelisting
  - Filtering out what you don't want
  - Only accepting what you expect
- But what to actually know to expect when you haven't got your information governance in order yet?
- ISO 27001: Risk based information security management systems

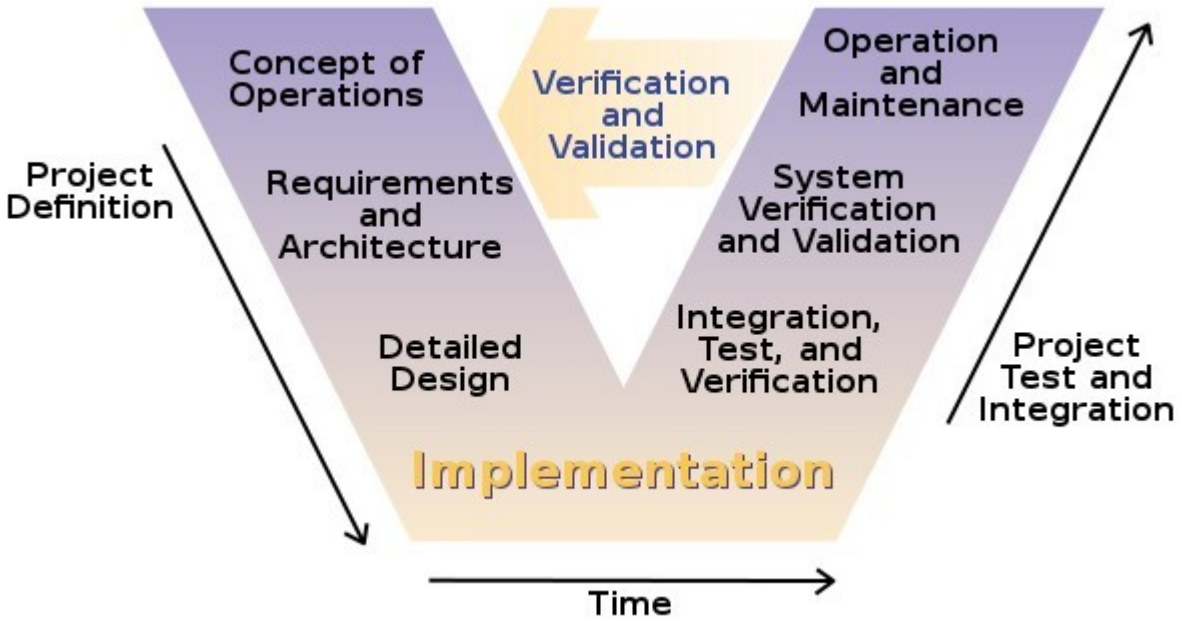


Industry example: Pharma / medical

- GAMP – Good Automated Manufacturing Practice (since 1990's)
  - Risk based computerized system lifecycle and validation management methodology
  - Goals (FDA / EMA specified):
    - Establish all risk vectors from the perspective of the patient
    - In clinical studies prevent adverse events (e.g. patients dying) and if an adverse event occurs be able to trace its origins and prevent further escalation to other trial subjects (e.g. patients)
  - Quite similar to healthy and mature information governance?
- Sidenote: Healthcare depends on IoT devices heavily
  - Hacking a pacemaker or insuline pump, what can go wrong?



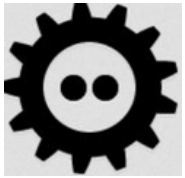
Evaluation / validation of free / open source software



OpenNovations by DevHdR

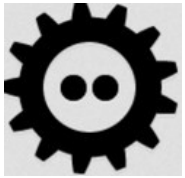
The General Data Protection Regulation

- Same principle, risk based approach
- Power to the people!
  - Or give back control over personal data
- Fundamental rights:
  - Right of access and transparency
  - Right to portability (e.g. export)
  - Right to demand erasure
- For companies: Information governance.
  - Single privacy authority instead of multiple national privacy authorities



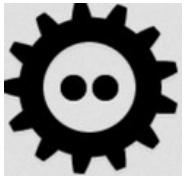
EU Competence network

- Focus on competence sharing and standardization
  - EU currently has no coherent ICT security competence management strategy
  - Individual national CERTS and competence centers are inward facing, limited EU cooperation
- ENISA will also play a centralized role
  - More focus on information security management instead of technical security measures.



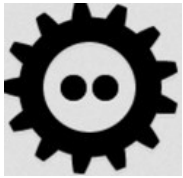
Upgrading security in education

- Hot topic in ICT courses in NL
  - Universities are scrambling to add Secure programming to the curriculum
    - Current materials include examples like:
      - <?php $userSql = “SELECT * FROM user WHERE username = “ . $_POST[‘username’] . “ AND password = “ . md5($_POST[‘password’]); ?>
  - Yes…. Really….. What can go wrong…?!?
- National news bulletins: >15 real life examples of courses with basic OWASP Top 10 mistakes...



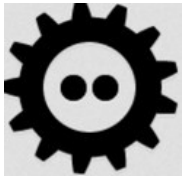
Cyber security certification

- ISO15408 – Information technology — Security techniques — Evaluation criteria for IT security:
  - Part 1: Introduction and general model
  - Part 2: Security functional components
  - Part 3: Security assurance components
- ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.



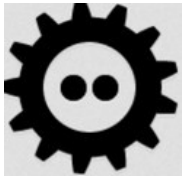
Voluntary certification scheme?

- The EU directive initiative states:
  - Recourse to European cybersecurity certification should therefore remain voluntary, unless otherwise provided in Union legislation laying down security requirements of ICT products and services.
- Voluntary / should? Like in the ISO 15408 “not required”?
  - ISO/IEC 15408 interprets “not necessarily required” to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.



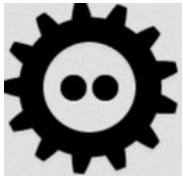
ISO15408: Part 1: Introduction and general model

- “TOE” (Target of Evaluation).
  - A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.



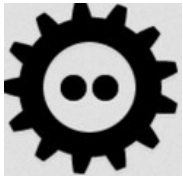
ISO15408: Part 1: Introduction and general model

- Examples of TOEs include:
  - A software application;
  - An operating system;
  - A software application in combination with an operating system;
  - A software application in combination with an operating system and a workstation;
  - An operating system in combination with a workstation;
  - A smart card integrated circuit;
  - The cryptographic co-processor of a smart card integrated circuit;
  - A Local Area Network including all terminals, servers, network equipment and software;
  - A database application excluding the remote client software normally associated with that database application.



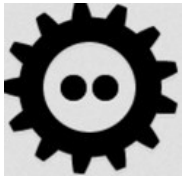
ISO15408: Part 1: Introduction and general model

- Different representations of the “TOE” (Target of Evaluation).
  - a list of files in a configuration management system;
  - a single master copy, that has just been compiled;
  - a box containing a CD-ROM and a manual, ready to be shipped to a customer;
  - an installed and operational version.
- Different configurations of the TOE?
  - As, during an ISO/IEC 15408 evaluation, it will be determined whether a TOE meets certain requirements, this flexibility in configuration may lead to problems, as all possible configurations of the TOE must meet the requirements. For these reasons, it is often the case that the guidance part of the TOE strongly constrains the possible configurations of the TOE.



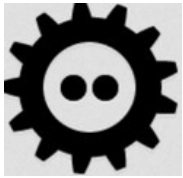
ISO15408: Part 1: Introduction and general model

- Target audiences for ISO15408:
  - Consumers
    - Create application / implementation independent requirements → “Protection Profiles” (PP)
  - Developers
    - Create implementation-dependent construct → the Security Target (ST)
  - Evaluators
  - Others



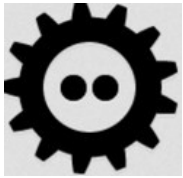
ISO15408: Part 1: Introduction and general model

- Chapters on:
  - 7 – Tailoring security requirements
  - 8 – Protection profiles and packages
  - 9 – Evaluation results
  - Annex A – Specification of security targets
  - Annex B – Specification of protection profiles
  - Annex C – Guidance to operations
  - Annex D – PP conformance



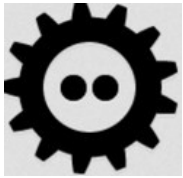
ISO15408: Part 1: Introduction and general model

- Chapter 7 – Tailoring security requirements
  - Iteration: allows a component to be used more than once with varying operations;
    - Refinement, hardening, etc.
  - Assignment: allows the specification of parameters;
    - “When” → “Then” (e.g. after >3 failed logins, user is blocked)
  - Selection: allows the specification of one or more items from a list; and
  - Refinement: allows the addition of details.



ISO15408: Part 1: Introduction and general model

- Chapter 8 – Protection profiles and packages
  - Protection profile
    - A Security Target (ST) always describes a specific TOE (e.g. the IPTables Firewall), a PP is intended to describe a TOE type (e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations.
  - Package
    - (Named) Set of (assurance / functional) security requirements.
      - SAR / SFR – Security Assurance (Part 2) / Functional (Part 3) Requirements



ISO15408: Part 1: Introduction and general model

- Chapter 9 – Evaluation results
  -

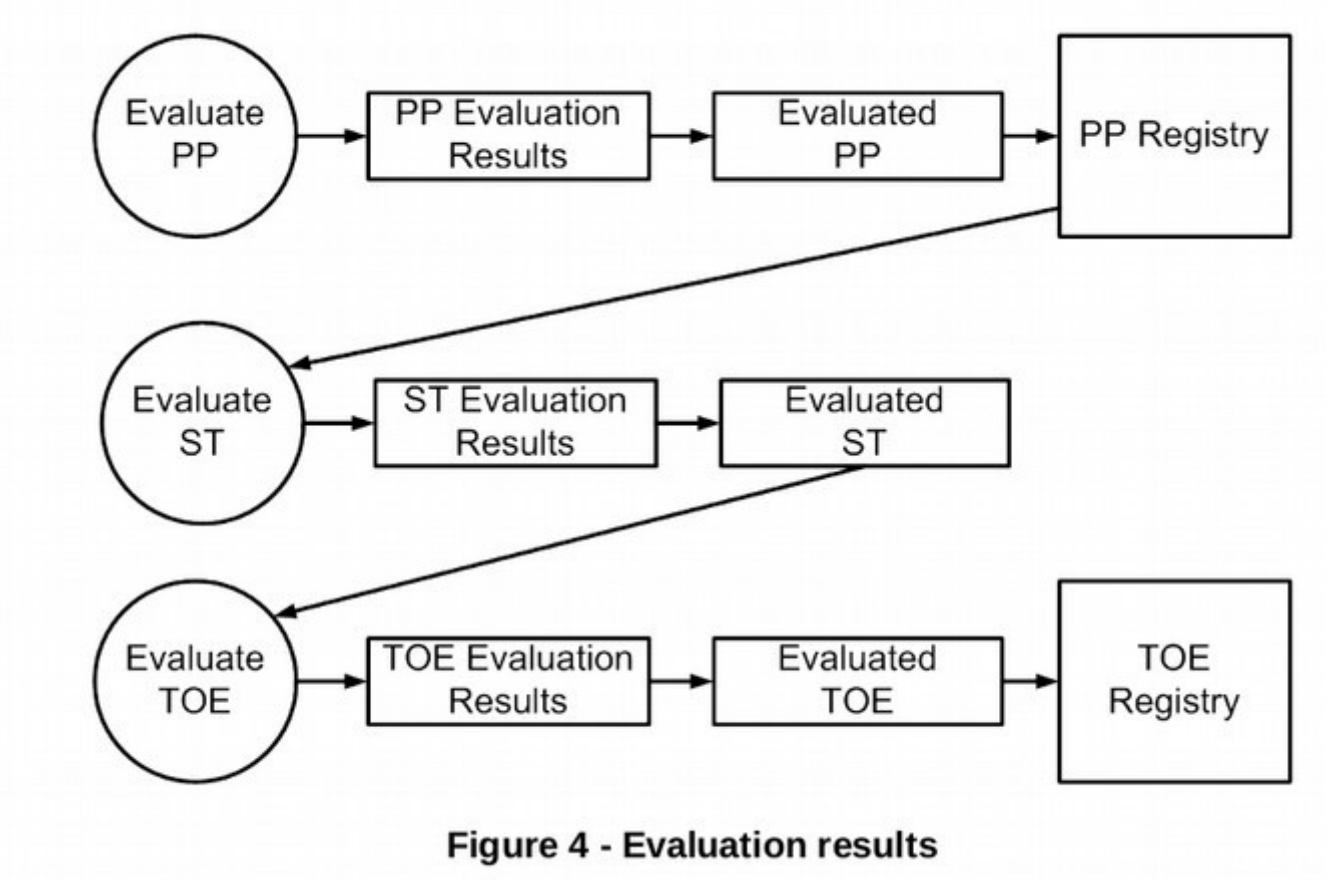


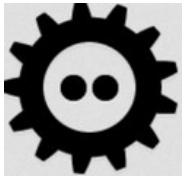
Figure 4 - Evaluation results

OpenNovations by DevHdR

ISO15048: Scope

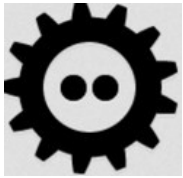
	Consumers	Developers	Evaluators
Part 1	Use for background information and are obliged to use for reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Are obliged to use for the development of security specifications for TOEs.	Are obliged to use for reference purposes and for guidance in the structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Are obliged to use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Are obliged to use for reference when interpreting statements of functional requirements.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use for reference when interpreting statements of assurance requirements.

Table 1 — Road map to the "Evaluation criteria for IT security"



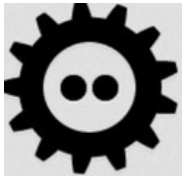
ISO15408: Assets and environments

- Assets are entities that someone places value upon.
- Examples of assets include:
  - contents of a file or a server;
  - the authenticity of votes cast in an election;
  - the availability of an electronic commerce process;
  - the ability to use an expensive printer;
  - access to a classified facility.
- but given that value is highly subjective, almost anything can be an asset.



ISO15408: Assets and environments

- The environment(s) in which these assets are located is called the operational environment. Examples of (aspects of) operational environments are:
  - the computer room of a bank;
  - a computer network connected to the Internet;
  - a LAN;
  - a general office environment



ISO15408: Concepts / relationships

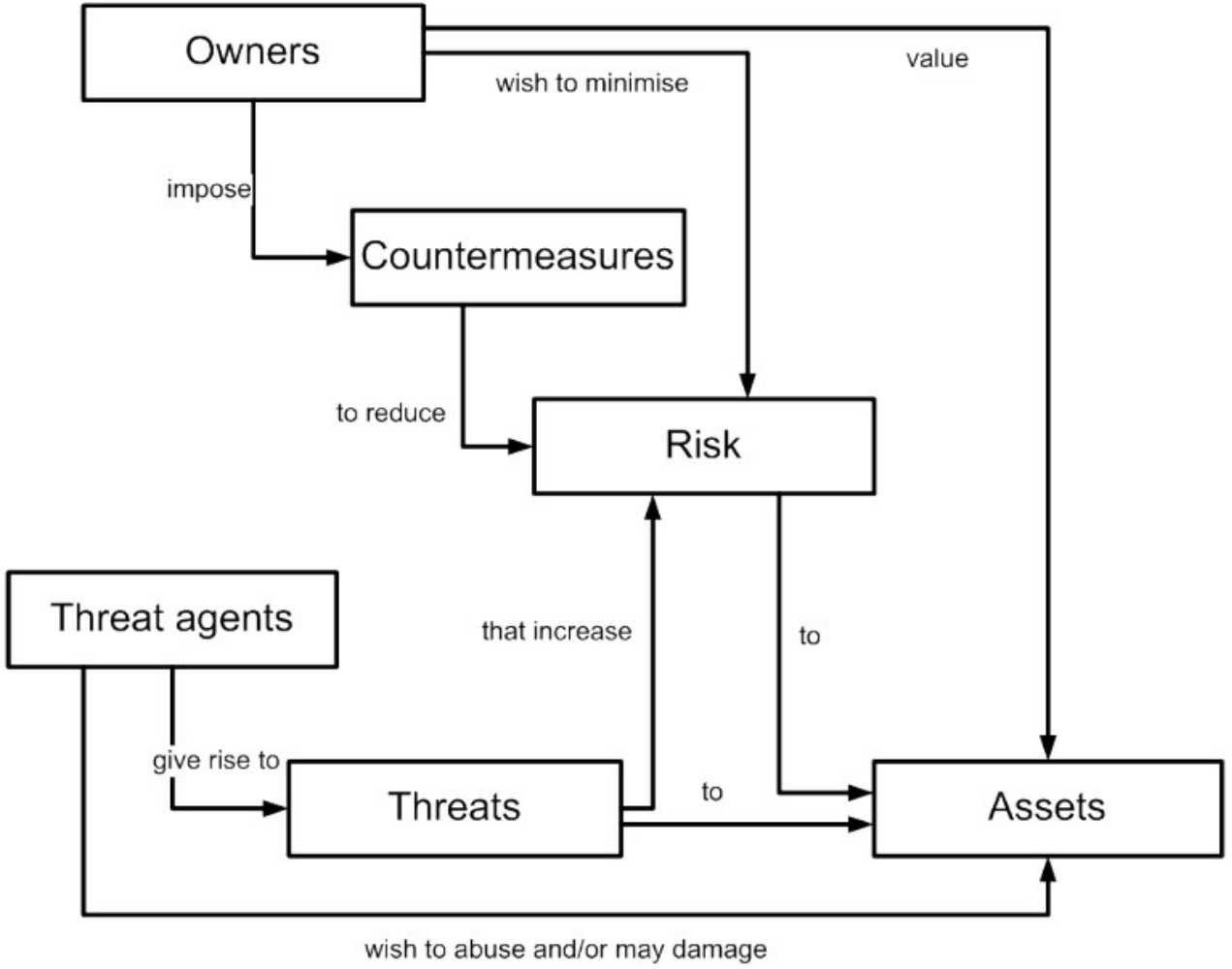
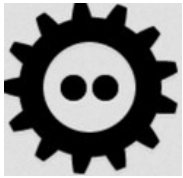


Figure 2 - Security concepts and relationships

OpenNovations
by DevHdR

ISO15408: Demonstrate fitness for purpose of measures

- Two important elements in defending this decision are being able to demonstrate that:
  - the countermeasures are sufficient: if the countermeasures do what they claim to do, the threats to the assets are countered;
  - the countermeasures are correct: the countermeasures do what they claim to do.



ISO15408: Evaluate fitness for purpose of measures

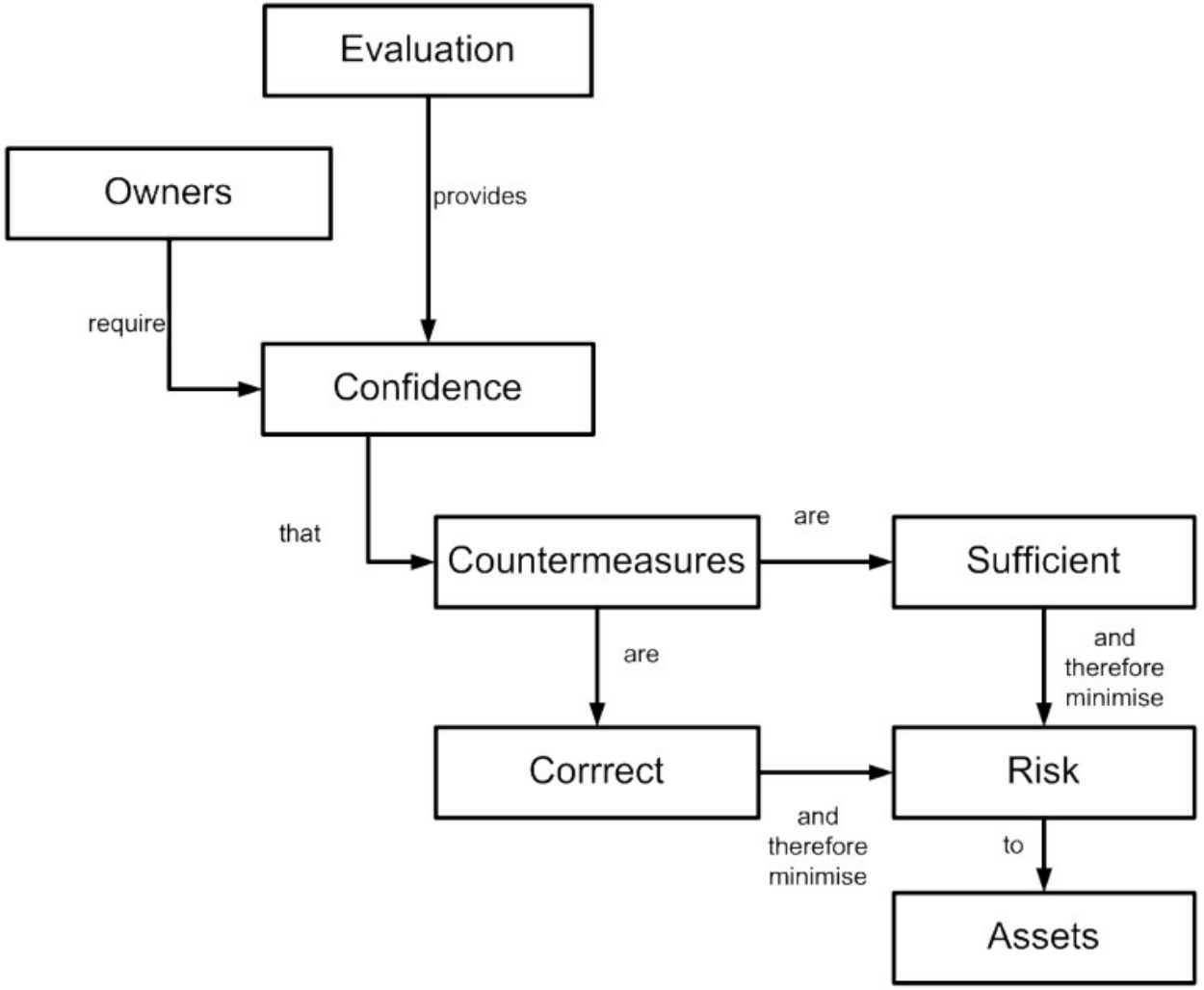
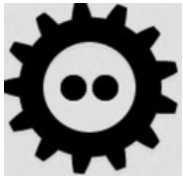


Figure 3 - Evaluation concepts and relationships

OpenNovations
by DevHdR

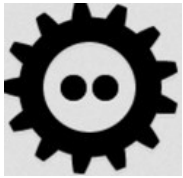
ISO15408: Part 2: Security functional components

- This part of ISO/IEC 15408 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.
  - Consumers
    - selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST.
  - Developers
    - respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part
  - Evaluators
    - who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied



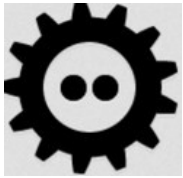
ISO15408: Part 2: Security functional components

- TOE (Target Of Evaluation) evaluation is concerned primarily with ensuring that a defined set of security functional requirements (SFRs) is enforced over the TOE resources.
  - The SFRs define the rules by which the TOE governs access to and use of its resources, and thus information and services controlled by the TOE.
  - SFRs may define multiple Security Function Policies (SFPs)
    - SFRs may define multiple Security Function Policies (SFPs) to represent the rules that the TOE must enforce



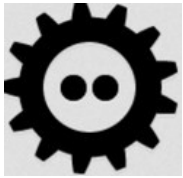
ISO15408: Part 2: Security functional components

- Each such Security Function Policy (SFP) must specify its scope of control, by defining the subjects, objects, resources or information, and operations to which it applies
- Those portions of a TOE that must be relied on for the correct enforcement of the SFRs are collectively referred to as the TOE Security Functionality (TSF).
  - The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.
    - Also for interfaces (TSFI) between TOE's.



ISO15408: Part 2: Security functional components

- Users, subjects, information, objects, sessions and resources controlled by rules in the SFRs may possess certain attributes that contain information that is used by the TOE for its correct operation.
  - Some attributes, such as file names, may be intended to be informational or may be used to identify individual resources while others, such as access control information, may exist specifically for the enforcement of the SFRs.
  - These latter attributes are generally referred to as “security attributes”.



ISO15408: Part 2: Security functional components

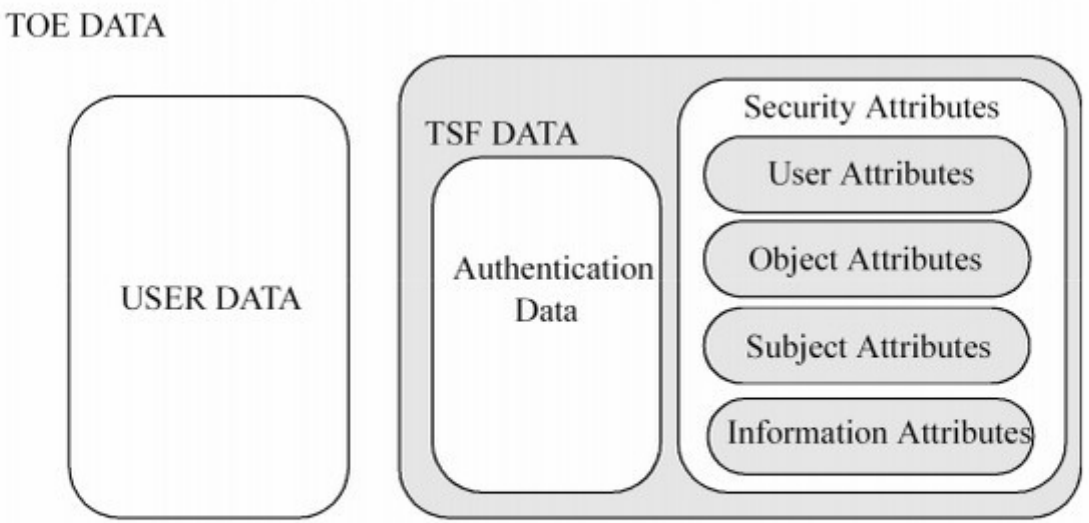
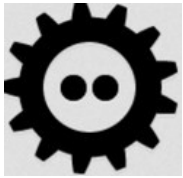


Figure 1 — Relationship between user data and TSF data

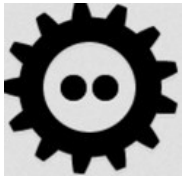
ISO15408: Part 2: Security functional components

- Functional requirement chapters
  - FAU: Security audit
  - FCO: Communication
  - FCS: Cryptographic support
  - FDP: Userdata protection
  - FIA: Identification and authentication
  - FMT: Security management
  - FPR: Privacy
  - FPT: Protection of the TOE Security Functionality (TSF)
  - FRU: Resource utilitisation
  - FTA: TOE access
  - FTP: Trusted path/channels



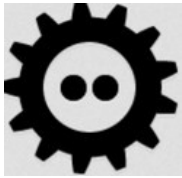
ISO15408: Part 3: Security assurance components

- This part of ISO/IEC 15408 defines the assurance requirements of ISO/IEC 15408.
  - It includes
    - the evaluation assurance levels (EALs) that define a scale for measuring assurance for component Targets of Evaluation (TOEs),
    - the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs,
    - the individual assurance components from which the assurance levels and packages are composed,
    - and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).



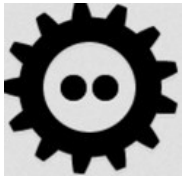
ISO15408: Part 3: Security assurance components

- Assurance approach
  - Vulnerabilities cause and significance
    - Vulnerabilities can arise through failures in:
      - a) requirements -- that is, an IT product may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;
      - b) development -- that is, an IT product does not meet its specifications and/or vulnerabilities have been introduced as a result of poor development standards or incorrect design choices;
      - c) operation -- that is, an IT product has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.



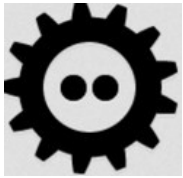
ISO15408: Part 3: Security assurance components

- Assurance approach
  - Vulnerabilities cause and significance
    - Vulnerability mitigation / management, to the extent feasible vulnerabilities should be:
      - a) eliminated -- that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;
      - b) minimised -- that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;
      - c) monitored -- that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.



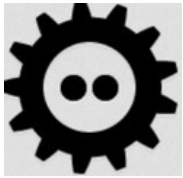
ISO15408: Part 3: Security assurance components

- Evaluation approach (examples):
  - a) analysis and checking of process(es) and procedure(s);
  - b) checking that process(es) and procedure(s) are being applied;
  - c) analysis of the correspondence between TOE design representations;
  - d) analysis of the TOE design representation against the requirements;
  - e) verification of proofs;
  - f) analysis of guidance documents;
  - g) analysis of functional tests developed and the results provided;
  - h) independent functional testing;
  - i) analysis for vulnerabilities (including flaw hypothesis);
  - j) penetration testing



ISO15408: Part 3: Security assurance components

- Evaluation assurance scale principles:
  - ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance.
  - The increasing level of effort is based upon:
    - a) scope -- that is, the effort is greater because a larger portion of the IT product is included;
    - b) depth -- that is, the effort is greater because it is deployed to a finer level of design and implementation detail;
    - c) rigour -- that is, the effort is greater because it is applied in a more structured, formal manner.



ISO15408: Part 3: Security assurance components

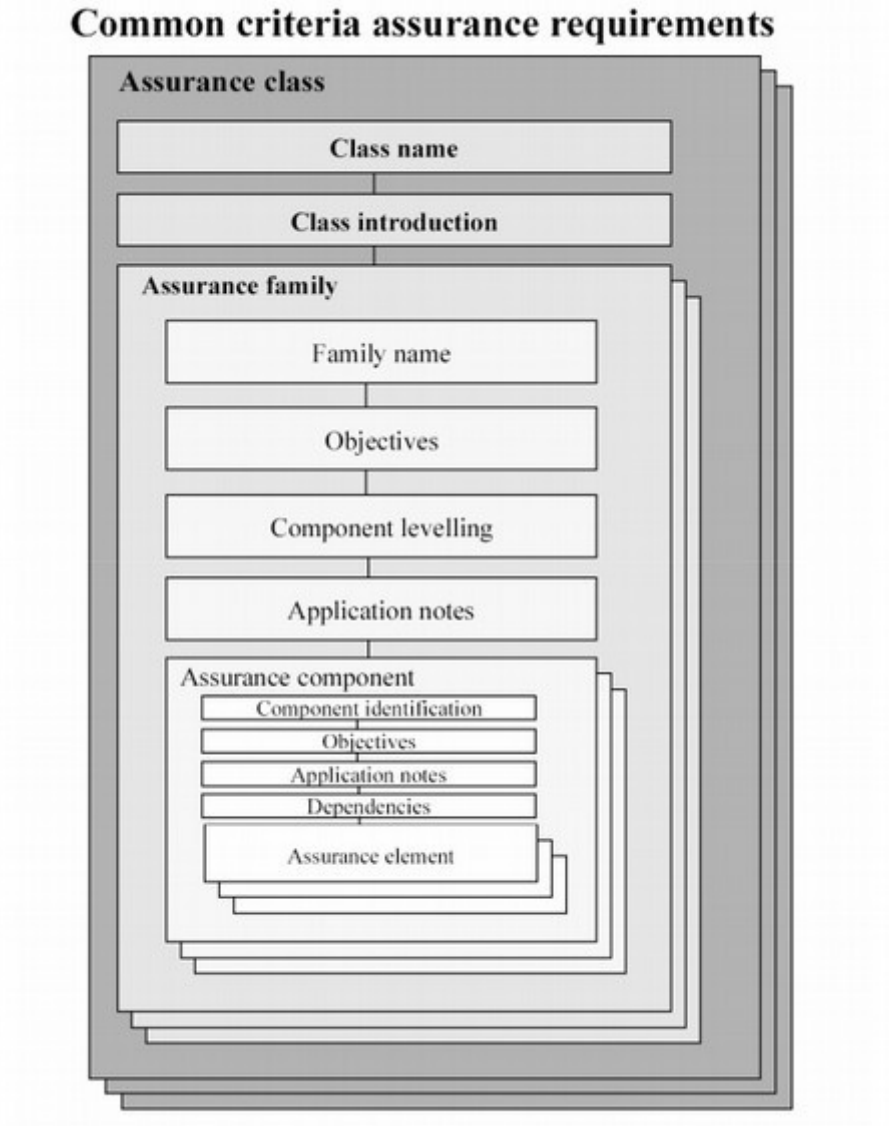
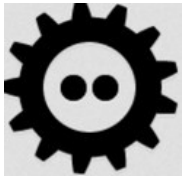


Figure 1 — Assurance class/family/component/element hierarchy

OpenNovations by DevHdR

ISO15408: Part 3: Security assurance components

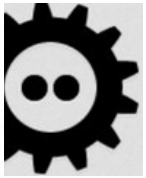
- Evaluation assurance levels (EAL)
  - 1 – Functionally tested
  - 2 – Structurally tested
  - 3 – Methodically tested and checked
  - 4 – Methodically designed, tested, and reviewed
  - 5 – Semiformally designed and tested
  - 6 – Semiformally verified design and tested
  - 7 – Formally verified design and tested



ISO15408: Part 3: Security assurance components

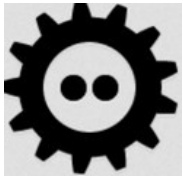
Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.4 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 8 — EAL7



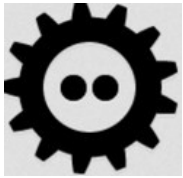
ISO15408: Part 3: Security assurance components

- Classes
  - APE: Protection profile evaluation
  - ASE: Security target evaluation
  - ADV: Development
  - AGD: Guidance documents
  - ALC: Lifecycle support
  - ATE: Tests
  - AVA: Vulnerability assessment
  - ACO: Composition



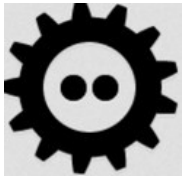
Relevance for free / open source software?

- Prepare to step up the security game
  - At least be aware of these legislative developments
- FOSS is a heterogenous ecosystem
  - Everything from hobby projects to enterprise grade communities
  - Yet projects are interdependent
  - Focus very dominantly on development related tasks
- Is FOSS outside of “the law”?



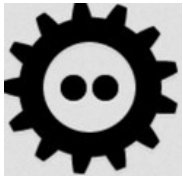
Evaluation / validation of free / open source software

- Validation = “demonstration of fitness for purpose”
  - Define purpose first (user requirements, functional / configuration specifications, etc)
  - Define validation criteria (test strategies, test cases, etc)
  - Ensure traceability between requirement / specification / testcase (validation → V-model)
- ISO15408 – for configurable systems, offer preconfigured scenario’s of usage to be evaluated
  - Community effort to create such standardized scenarios (Protection Profiles)?



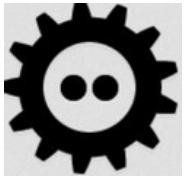
FOSS and GDPR?

- Personal data?
  - Logins, email addresses, etc?
  - Self hosted SCRMS (git)?
- But, who to address?
  - Open source community governance foundations / cooperations
    - SUSE Gmbh? Drupal Association? FSFE? Etc?
  - What to do on an incident? Data-breach?
    - Who to penalize if all goes south?



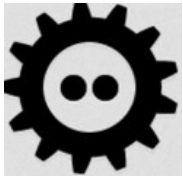
We still have time!

- Communities do need to start organizing though
  - Even though FOSS exists in a mainly virtual environment
  - That doesn’t mean that we operate outside the law
- We can also benefit from this
  - Shift from marketing driven SaaS (“Safe harbor”, “Privacy Shield” <> GDPR?)
  - Collaboration on co-created validation packages can benefit a whole community
    - Just like testing, documentation, etc does.



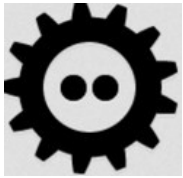
Who already has ISO15408 certificaction?

- Amongst others (RH): SUSE!
  - Common Criteria Security Certifications
  - SUSE received Common Criteria Certificates at Evaluation Assurance Level EAL4, augmented by ALC_FLR.3 (EAL4+) for SUSE Linux Enterprise Server 12 BSI-DSZ-CC-0962-2016 and SUSE Linux Enterprise Server 11 SP2 (BSI-DSZ-CC-0787-2013 and BSI-DSZ-CC-0852-2013) including KVM virtualization on x86_64 and IBM System z. To achieve the certifications, the SUSE products and processes for developing and maintaining its products passed a rigorous security evaluation performed by atsec information security. The certificates were issued by Bundesamt für Sicherheit in der Informationstechnik (BSI). the German Federal Office for IT Security. The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) recognized by 26 countries worldwide.
  - https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Betriebssysteme/0962.html



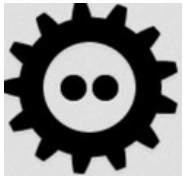
What to do?

- Adopt terminology regarding system descriptions
  - Security targets, Protection Profiles, Security Functional Requirements, etc
- Create work packages in repositories for security experts / evaluators to contribute to
  - Create templates for Security Target/Protection profiles, etc, just like bug/issue reporting templates
- Describe the purpose of a system / application / library to allow demonstration of fitness for purpose
  - Not all systems have to implement NATO grade security policies.



Benefits and opportunities

- Easier adoption of FOSS in regulated environments
  - Hints, these are environments with big budgets (pharma, government, etc)
    - Money does help to support development
  - Actually FOSS is a big advantage due to the intrinsical opportunity for auditability
    - More eyes mean better quality
- What's there not to like?



Happy ending!