您的客户提出任何合规要求，我们都能按同一套方法落实。

无论是中国的等保2.0和《网络安全法》、香港第 653 章，还是欧盟法规或国际标准，我们都把要求转化为一套统一的控制措施，并交付可供审查的证据。软件、物联网与自动化项目自 2009 年起交付。

一次建设，多法规适用
同一项控制措施同时满足多部法规，避免重复投入。

证据先行
每一步都产出文件，可直接交给客户、测评机构或审核方。

中欧两端都懂
项目在中国合规，同时符合欧洲客户的期望。

五个步骤，适用于所有法规

1. **范围与要求清单**
   产出：要求登记表
2. **映射到统一控制集**
   产出：对照矩阵
3. **架构与控制措施**
   产出：安全架构、威胁模型
4. **证据包**
   产出：技术文件、测试报告、SBOM、声明
5. **运营：报告与更新**
   产出：事件报告流程、漏洞与更新流程

一项控制措施，对应多部法规（节选）

控制措施	中国 等保2.0 / 网络安全法	香港第 653 章	IEC 62443	ISO/IEC 27001:2022	欧盟 CRA
访问控制与强身份鉴别	安全计算环境：身份鉴别、访问控制	《工作守则》	4-2 CR 1.1、CR 2.1	A.5.15、A.8.5	附件一 (2)(d)
签名更新与安全启动	安全计算环境：可信验证	《工作守则》	CR 3.4、3.10、3.14	A.8.19、A.8.32	附件一 (2)(c)(f)
漏洞处理与 SBOM	安全运维管理：漏洞和风险管理	《工作守则》	4-1 DM、SUM	A.8.8	附件一 第二部分
安全事件报告	4 小时（关基：1 小时）	严重事故 12 小时，其他 48 小时	2-1 事件响应	A.5.24–A.5.26	24 小时 / 72 小时
风险评估与审核	定级备案、等级测评（三级：每年）	每年风险评估，每两年独立审计	3-2	条款 6.1.2、8.2	第 13 条

截至 2026 年 11 月，已简化。香港第 653 章直接适用于被指定的关键基础设施营运者，其供应商通过营运者的要求来满足。

完整示例作为证明

欧盟《网络弹性法案》(CRA) 完整示例，参考博世力士乐、菲尼克斯电气、西门子和库卡的公开做法。免费申请：**www.qmisoft.com/zh/examples/**

6 + 6 套参考方案 · 欧盟 · 内地 · 香港对比 · 10 张图表 · 4 套中英模板 · 63 个文件



施恒信 Herbert Schrank
创始人、软件架构师 · DI(FH) 工程硕士（应用科学大学）

- 自 2009 年起交付软件项目：从数据库、Web 应用到 PLC 与机器
- AI Tinkerers 成员（维也纳、香港）· AAIF 深圳社区 · 2026 年 10 月赴深圳展会
- 公司位于欧盟（奥地利）· 英文/德文沟通，文件提供中文版 · 报价按项目范围

微信扫码添加
info@qmisoft.com
+43 664 1935195

Whatever compliance requirement your customer sets, we implement it with one method.

China's MLPS 2.0 and Cybersecurity Law, Hong Kong Cap. 653, EU regulations or international standards: we turn each requirement into one shared set of controls and deliver evidence that can be reviewed. Software, IoT and automation projects since 2009.

Build once, comply many times
The same control answers several rulebooks, so you do not pay twice.

Evidence first
Every step ends with a document for your customer, test centre or auditor.

At home in China and Europe
Your project meets Chinese law and European customer expectations.

Five steps, the same for every rulebook

1. **Scope and requirements**
   Result: requirements register
2. **Map to one shared control set**
   Result: mapping matrix
3. **Architecture and controls**
   Result: security architecture, threat model
4. **Evidence pack**
   Result: technical file, test reports, SBOM, declarations
5. **Operate: report and update**
   Result: incident runbook, vulnerability and update process

One control, many rulebooks (extract)

Control	China MLPS 2.0 / CSL	Hong Kong Cap. 653	IEC 62443	ISO/IEC 27001:2022	EU CRA
Access control, strong login	Secure computing environment: identification, access control	Code of Practice	4-2 CR 1.1, CR 2.1	A.5.15, A.8.5	Annex I (2)(d)
Signed updates, secure boot	Secure computing environment: trusted verification	Code of Practice	CR 3.4, 3.10, 3.14	A.8.19, A.8.32	Annex I (2)(c)(f)
Vulnerability handling, SBOM	Security operations: vulnerability and risk management	Code of Practice	4-1 DM, SUM	A.8.8	Annex I Part II
Incident reporting	4 h (critical infrastructure: 1 h)	12 h serious, 48 h other	2-1 incident response	A.5.24–A.5.26	24 h / 72 h
Risk assessment and audit	Grading, filing, assessment (level 3: yearly)	Assessment yearly, independent audit every 2 years	3-2	Clauses 6.1.2, 8.2	Art. 13

As of Nov 2026, simplified. Cap. 653 binds designated critical-infrastructure operators; suppliers meet it via the operator's requirements.

A complete worked example as proof

EU Cyber Resilience Act (CRA), built on the published practice of Bosch Rexroth, Phoenix Contact, Siemens and KUKA. Request it free: **www.qmisoft.com/examples/**

6 + 6 reference concepts · **EU • China • HK compared** · **10 diagrams** · **4 templates EN/中文** · **63 files**



Herbert Schrank 施恒信
Founder & Software Architect • DI(FH), Master of Engineering

- Delivering software since 2009: from database and web apps down to PLCs and machines
- AI Tinkerers member (Vienna, Hong Kong) • AAIF Shenzhen community • Shenzhen fairs, Oct 2026
- EU-based (Austria) • English or German, documents also in Chinese • quoted per scope

Scan to add on WeChat
info@qmisoft.com
+43 664 1935195