Examples of cybersecurity culture
网络安全文化样本

Examples indicative of a weak cybersecurity culture 表明网络安全文化薄弱的样本	Examples indicative of a strong cybersecurity culture 表明网络安全文化强大的样本
Accountability for decisions related to cybersecurity is not traceable. 与网络安全有关的决策责任是不可追溯的。	The process ensures that accountability for decisions related to cybersecurity is traceable. 有流程确保与网络安全有关的决策责任是可追溯的。
Performance (of the implemented functionality or feature), cost or schedule take precedence over cybersecurity. （实现功能或特性的）绩效、成本或计划优先于网络安全。	Cybersecurity and safety have the highest priority. 网络安全和安全享有最高的优先级。
The reward system favours cost and schedule over cybersecurity. 奖励体系倾向的是成本和计划，而非网络安全。	The reward system supports and motivates the effective achievement of cybersecurity and penalizes those who take shortcuts that jeopardize cybersecurity. 奖励体系支持和激励网络安全的有效的业绩，并惩罚那些采取对网络安全有危害的捷径的人。
Cybersecurity personnel force inappropriate and very strict adherence to cybersecurity without considering specific needs of projects/activities. 网络安全人员不考虑项目或活动的具体需求，而采取不当的迫使和非常严格的方式来要求遵守网络安全。	Cybersecurity personnel act as role models with a good sense for appropriateness and practical implementation that leads to trust in their actions by the entire organization. 网络安全人员充当榜样，具备良好意识，保持恰当的和实际有效的执行行为，从而让整个组织信任他们的行为。
Personnel assessing cybersecurity and its governing processes are influenced unduly by those responsible for executing the processes. 网络安全评价人员和网络安全管理过程受到负责过程执行人员的过度影响。	The process provides adequate checks and balances, e.g. the appropriate degree of independence in cybersecurity assessment. 流程提供了合适的制衡，如，在网络安全评价中的适当程度的独立性。
Passive attitude towards cybersecurity, e.g.: 对网络安全的消极态度，如： — heavy dependence on testing at the end of the development; — 过分依赖开发末尾阶段的测试； — not being prepared for potential weaknesses or incidents in the field; — 没有为潜在弱点和现场事件做好准备； — management reacting only when there is a cybersecurity incident in production, in the field or if there is a lot of attention in the media about competitor products. — 管理层仅仅在生产和现场有网络安全事件，或媒体上对竞争对手产品有大量关注时才会做出反应。	Proactive attitude towards cybersecurity, e.g.: 对网络安全的积极态度，如： — cybersecurity issues are discovered and resolved from the earliest stage in the product lifecycle (cybersecurity by design); — 网络安全问题在产品生命周期最早阶段发现和处理（网络安全设计）； — the organization is prepared to react fast to vulnerabilities or incidents in the field. — 组织对漏洞或现场事件做出快速反应。
The required resources for cybersecurity are not allocated. 没有分配网络安全所需资源。	The required resources for cybersecurity are allocated. Skilled resources have the competence commensurate with the activity assigned. 分配了网络安全所需资源。专业人员具备胜任所承担活动的能力。
— “Groupthink” confirmation bias (i.e. uncritical acceptance or conformity to prevailing points of view). — “群体决策”的确认偏差（如，不加批评的接受或遵循主流观点）。 — “Stacking the deck” (i.e. choose members to ensure desired outcome) when forming review groups to prevent potential dissention. — “事先做牌”，当组建评审小组来防止潜在分歧时（如，选择成员确保预期结果）。 — Dissenter is ostracized or labelled as “not a team player” (e.g. uncooperative, intransigent, toxic person). — 异见者被排斥或被贴上“不合群”的标签（如，不配合、不服从、有毒的人）。 — Dissent reflects negatively on performance reviews. — 异议会对绩效考核产生负面影响。 — Minority dissenter is labelled or treated as a “troublemaker”, “not a team player” or a “whistle blower” (i.e. agitator, undesirable or a snitch). — 少数持不同意见的人被贴上“麻烦制造者”、“没有团队精神”、“不是一条心”的标签（如，煽动者、不受欢迎的或告密者）。 — Employees who express concerns fear repercussion. — 表达了担忧的员工害怕后果。	The process uses diversity to its advantage: 流程使用了多样化的优势： — intellectual diversity is sought, valued and integrated in all processes; — 知识多元化是被追求的，被尊重的以及被整合到组织所有流程中。 — behaviour which counters the use of diversity is discouraged and penalized. — 反对多样化使用的行为是不被鼓励的和要遭受惩罚的。 The supporting communication and decision-making channels exist and the management encourages their usage: 有配套的沟通和决策渠道，并且管理层鼓励这些渠道的使用： — self-disclosure is encouraged; — 自我表露是被鼓励的； — responsible disclosure by anyone (internal or external) of potential vulnerability is encouraged; — 鼓励任何人(内部或外部的)负责任地披露潜在的漏洞。 — the discovery and resolution process continues in the field, in manufacturing and in development of other products. — 发现和解决流程持续存在于该领域，存在于其他产品的生产和开发阶段。
No systematic continuous improvement processes, learning cycles or other forms of lessons learned. 没有系统化的持续改进流程、学习周期和其他形式的经验教训学习。	Continuous improvement is integral to all processes. 持续改进整合到了所有流程。
Processes are ad hoc or implicit. 流程是临时的或不明确的。	Defined, traceable, and controlled processes are followed. 已确定的、可追溯的和已受控的流程被遵循。