# "Who Watches the Watchmen?": A Critical Analysis of British Standards Concerning Security and Trust

**Group 4**

*[date]*

## Part I

# BS 10754–1:2018 or: How The British Standards Institution Learned to Stop Worrying and Copy NIST's Homework

The Cybersecurity Framework 1.0, published by the US Department of Commerce's (DoC) National Institute of Standards and Technology (NIST), is internationally recognised as the benchmark standard for establishing effective cybersecurity policies, across the public and private sectors. Originally published in 2014, the framework categorises cybersecurity risk assessment and management under five broad functions: identify, protect, detect, respond and recover. A revised version of the publication, the NIST Cybersecurity Framework 1.1 was published in 2018, shortly after the publication of the Information Technology–Systems Trustworthiness Part 1: Governance and Management Specification document (BS 10754–1:2018) by the British Standards Institution (BSI) in the same year. The two documents bear remarkable resemblance and in light of this, the following blog post will observe the commonalities between the two documents while critically assessing the risk assessment and management approach of BS 01754–1:2018, in the context of the security use case of cyber–physical systems (CPS).

It is important when discussing any kind of security to clarify terminology. Cybersecurity possesses a unique and extensive nomenclature and to ensure the accessibility of this blog post, we will be using it minimally. However, two core concepts for cybersecurity, trust and composition, are crucial to define for the context of this piece. The sociological definition of trust, which has been widely adopted by the cybersecurity community, is the reliance on an entity to behave as expected, despite its capacity to defy those expectations. In the context of this blog post, if a system were to behave as expected, only expected kinds of processing or computation would occur. Composition is the primary engineering approach to construct complex systems by composing preexisting components in layered designs. While the properties of individual components may be known and understood, the same properties of a combined system may be more difficult to ascertain, potentially resulting in unexpected behaviours.

BS 10754–1:2018 categorises risk assessment as "Understanding general risks" (6.3.2) and "Understanding trustworthiness risks" (6.3.3), though one may argue these are one and the same in the context of cybersecurity. The first section, "Understanding general risks", outlines the steps necessary to critically assess the composition of systems, which is consistent with the NIST Cybersecurity Framework (ID.RA) and the NIST Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (NIST SP 800–53 Rev. 4). To "assess the risk to trustworthiness", identifying and enumerating assets and their threats and vulnerabilities, which collectively manifest risks for systems, is asserted as sound methodology. This is consistent with the "Identify" section of the NIST Cybersecurity Framework, specifically subsections ID.AM, ID.R–3 and ID.R–1, respectively. The techniques listed to understand "general risks" may be considered vague and lacking technical specificity, which may indicate a lack of stakeholder engagement with the technical community.

The second section, "Understanding trustworthiness risks", outlines a rudimentary threat intelligence framework to identify threats and vulnerabilities, utilising common cybersecurity resources such as the Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) databases. While these databases are important resources for intelligence–gathering, this might be described as a "minimum viable framework" for threat intelligence. Indeed, it excludes common intelligence–gathering methods for cybersecurity, such as monitoring activity on threat actor strongholds such as darkweb forums and internet relay chat (IRC) channels. Additionally, in the context of cyber–physical systems, monitoring and analysing data collected from the Shodan search engine and the US DoC's Centre for Applied Internet Data Analysis (CAIDA) network telescope is common practice for intelligence–gathering concerning Internet of Things (IoT), CPS and industrial–control systems (ICS). This is not included in the document, further indicating a lack of critical stakeholder engagement. Again, all of the proposed steps are consistent with the NIST Cybersecurity Framework (ID.RA–2) and NIST SP 800–53 Rev. 4.

BS 10754–1:2018 categorises risk management as "Controls" (6.4), under the subheadings of personnel (6.4.2), physical (6.4.3), procedural (6.4.4) and technical (6.4.5). It would be impossible to [word] all of the recommendations in this piece, however several particularly egregious recommendations bear scrutiny. The recommendation for a "single accountable owner of people risk" (PE.03.10) would create a single point of failure, meaning if that party were compromised, it would likely result in loss of trust across the entire workforce The final category, Technical Controls, contains the most problematic content, for example, "Selection of appropriate programming languages, considering known vulnerabilities" (TE.02.10). This may be considered an ill–informed statement, as most modern programming languages are Turing–complete, meaning they can approximately simulate the computational processes of any other programming language, thus rendering the point moot. Other recommendations such as "Select appropriate algorithms" (TE.04.30) and "Integrate and configure components" (TE.07.50) offer no particular insight, further exacerbating the impression that the document was not written by a technically proficient author(s). Other examples include removing "any unused functions, macros, formats, codes, etc." (TE07.70) and "temporary files / logs" (TE.08.55), thus destroying valuable forensic evidence in the event of an incident, and storing source code with an escrow service (TE.11.10), thus increasing the composition, and attack surface, of a system.

On the balance of evidence, we assert that BS 10754–1:2018 provides little meaningful value over and above the NIST Cybersecurity Framework, of which it appears largely derivative. Its content reflects lack of stakeholder engagement, particularly with the technical community, and although it is intended as a high–level document, its recommendations are generally reductive and lack technical specificity to such a degree that it impacts the document's credibility. As such, we find BS 10754–1:2018 to be inadequate

with regards to providing effective recommendations for ensuring the trustworthiness of information and communication technology systems, including CPS.

## Part II

# Managing The Risks of Composition

In this section, we will critically analyse two risk assessment methods proposed in the Risk Management – Risk Assessment Techniques standard (IEC 31010:2019), published by the International Organization for Standardization (ISO) Risk Management Technical Committee (ISO / TC 262) in 2019. In congruence with the topic of this piece, we have selected [**method1**] and [**method2**], as they are salient to the security issues concerning system composition (See **INTRODUCTION**).