2 Introduction, overview, and document structure

This is the security metrics book, a vital component of CISO efforts to measure performance and optimize protection.

Enterprises measure programs in order to manage them. This book provides business metrics for a CISO to measure their protection program. As such, it provides a feedback mechanism designed to help the CISO guide the enterprise protection program.

Technologists often measure things available to them and try to position them as indicative of progress. This includes things like number of vulnerabilities found and eliminated, systems inspected, or incidents investigated. But these are really just examples of “building a ramp to the moon”.

> *Imagine someone tells you they want to build a ramp to the moon. The plan is to build a big ramp and climb it to get to the moon. The plan uses proven technology and there is clear progress every day. The first day the ramp is 10 meters high and that makes us 10 meters closer to the moon. On they go, getting closer to the moon every day. Process improvements lead to progress of 30 meters in one day.*

Presumably everyone sees the logical flaw in this approach, you cannot solve this problem with this solution, even though you can make apparent progress every day and report stunning figures for years. The nature of the security problem is similar to the nature of building a ramp to get to the moon. You will never reach the moon and you will never get “secure”.

A meaningful metric for an enterprise security program has to:

1. make sense in terms of some objective,
2. be relevant to the issues at hand to the enterprise,
3. be quantifiable in relative terms, and
4. be associated with cost in some way.

Based on the CISO Governance Guidebook, this book provides management measures of the enterprise protection program at the level of the CISO. It uses standards and Governance Guidebook to help measure the effectiveness and progress of the protection process. It is broken into different perspectives to allow different approaches to be taken depending on the preference of the CISO and to allow portions of the overall book to be selectively applied to elements of a program or as top level views for further drill-downs.

2.1 Using the metrics

The metrics are provided in two general forms. Either an item is Yes/No (YN), Low/Medium/High (LMH) or rated from 0 to 10. Everything item and issue is stated as a declarative statement, like “The book is red”.

- For YN entries a Yes indicates that the statement is always True.
- For LMH entries, look at the explanation in place.
- For 0 to 10 ratings the statement is rated in two parts:
  - Part 1: What portion of the relevant examples is it true for?
  - Part 2: How true is it for each example?

Example:

The declarative statement:

Organizational structures provide the CISO influence or control over all organizational and business process areas.

Rating from 0 to 10.

Part 1: Out of the list of major areas identified for the influence or control of the CISO, the CISO has no influence over Legal, HR, Audit, or Documentation. This is 4 out of 10 areas, so the portion of relevant examples would be 60% or 0.6.

Part 2: The level of influence of the CISO in the areas over which there is substantial influence is: (1) complete control over the awareness program (100%), (2) almost complete control over the change control program (90%), and (3) shared control over the rest of the areas (50%), or an average of (1+0.9+(0.5*4))/6 = 3.9/6 or about 65% or 0.65.

The rating is then 0.6*0.65=0.39/1 or 3.9 on a 0 to 10 scale.

At the end of each major area there is an additional chart that looks like this:

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	6	7	9.5

This comparison chart is designed to put results in context. There are 5 different values provided:

1. Startup: indicates how typical protection programs rate when the program is evaluated just as the CISO is put in place.
2. Diligence: indicates what would be expected to meet due diligence requirements, indicating what is reasonable and prudent as a minimal level of achievement.

3. Typical: indicates what a typical program rates after operating for something like 3 to 5 years under steady funding and reasonably good management.
4. Excellent: indicates what a program with high expectations and strong management support operating over the long term achieves.
5. Best: indicates what the best programs achieve.

Taking our example, the rating is higher than the average information protection program at its inception but falls shy of due diligence by quite some way. Given the information about how this rating came to be, the quickest way to reach due diligence levels would be to gain some reasonable level of influence over the HR, Legal, and Audit processes, which would immediately bring the rating into the typical range.

A similar approach can be taken to the Yes/No and True/False areas which have scores that are composed of several answers. If there are 2 True/Yes answers out of 10 and due diligence requires a rating of 4 out of 10, reaching a level of due diligence can be achieved by finding a way to make two more of these items true. If one of the items is usually true but not always, it might be easier to make it always true than to try to get one that is almost never true to be always true.

As a rule of thumb, a sound approach to using this book for program tracking and improvement is to:

1. choose the desired objectives of the enterprise in terms of the comparison chart.
2. Based on existing ratings, determine what improvements are easiest, most desirable, or most cost effective.
3. Implement those improvements in the desired time frame, remeasure, and declare success in achieving your objectives.

Reaching levels indicated in this book is no guarantee that other independent evaluators will agree with the results. Just because you have taken specific steps and made specific choices to try to reach an objective against the metrics provided here does not mean that every auditor will agree with the evaluation or the approach. But the book is useful in countering claims by independent evaluators and auditors with regard to your program. When they say that they think that elements of your program are inadequate, these metrics can be powerful tools in asking them what they have found other enterprises achieve and in identifying specific areas where they think emphasis should be put.