Ensuring Operational Audit Of Critical Information Infrastructure Management Systems

Livshitz Ilya
ITMO University, IT-Security faculty, Russia

+7 (921) 934-48-46
Livshitz.il@yandex.ru

1. Introduction

- Problem of ensuring the effectiveness of audits is partly caused by the frequently changing approaches to certification, the periodic and **not always synchronized** releases of new international standards and their accurate and literally translations.
- The expert community, as a rule, use a simple formal procedures, especially if external certification bodies strictly adhere to the standard **3-year certification cycle.**
- Accordingly, many companies "inherit" the same formal practice and similarly establish a fixed cycle for their own **internal audit programs**. How applicable is this in today's environment?

2. Certification statistics data. World

	Number of certificates in 2023	Number of certificates in 2024	Difference	Variation in %
ISO 9001:2015	837 978	1 474 118	636 140	76%
ISO 14001:2015	300 410	676 232	375 822	125%
ISO 45001:2018	185 166	542 527	357 361	193%
ISO/IEC 27001:2013&2022	47 291	96 709	49 418	**104%**
ISO 50001:2018	24 924	38 482	13 558	54,4%

2. Certification statistics data. Russia

Land/Sector	Electrical and optical equipment	Transport, storage and communication	Information technology	Engineering services	Sector unknown
Russian Federation (the)	**1**	**1**	**6**	**1**	**44**

Country	Number of certificates in 2023	Number of certificates in 2024	Difference	Variation in %
Russian Federation (the)	**25**	**53**	**28**	**112 %**

3. Research method and problem statement

The mathematical formulation of the problem is presented below as a general optimization problem with basic sets that characterize the properties of a specific CII:

$$< X; R; C; F> \rightarrow Y \qquad (1)$$

X – a set of input parameters (for example, the number of divisions and personnel);
R – a **risk profile (residual risks)** for the audited MS;
C – a set of constraints (for example, cost, time, and qualified auditors);
F – a set of variables (for example, the **frequency of audits** and the number of auditors);
Y – a set of output parameters (for example, cost-effectiveness).

3. The method of standard (fixed) audits

Taking into account the formulation of the task, we will determine the parameters of the standard audit method, which exactly meets the formal requirements of the applicable standards (specified above), takes into account the requirements of general audit standards (ISO 19011 and ISO/IEC 17021-1), and is focused on a **fixed annual audit cycle**.

Parameter	Evaluation	Status	Consequence
X	Not considered	Fixed	-
R	High residual risk	Fixed	**Negative impact of the risk**, as there is a long time (maximum one year) between the identification and "closure" of the discrepancy
C	A significant opportunity	Fixed	A significant cost saving opportunity, as periodic formal participation by mid-level auditors is required
F	Average opportunity	Fixed	Average savings potential, as there is a fixed frequency of audits and periodic formal participation of mid-level auditors
Y	High residual risk	Fixed	**Negative impact of the risk**, as there is a long time (maximum one year) between the identification and "closure" of the discrepancy, but some critical incidents can be closed more quickly

4. The method of operational audits

The idea of applying not a fixed, but a variable dynamic process of audit of various MS was first proposed by the author in the dissertation in 2018. This intention does not align with the practice of standard “fixed” audits, which has not undergone any process innovations over the past 10 years.

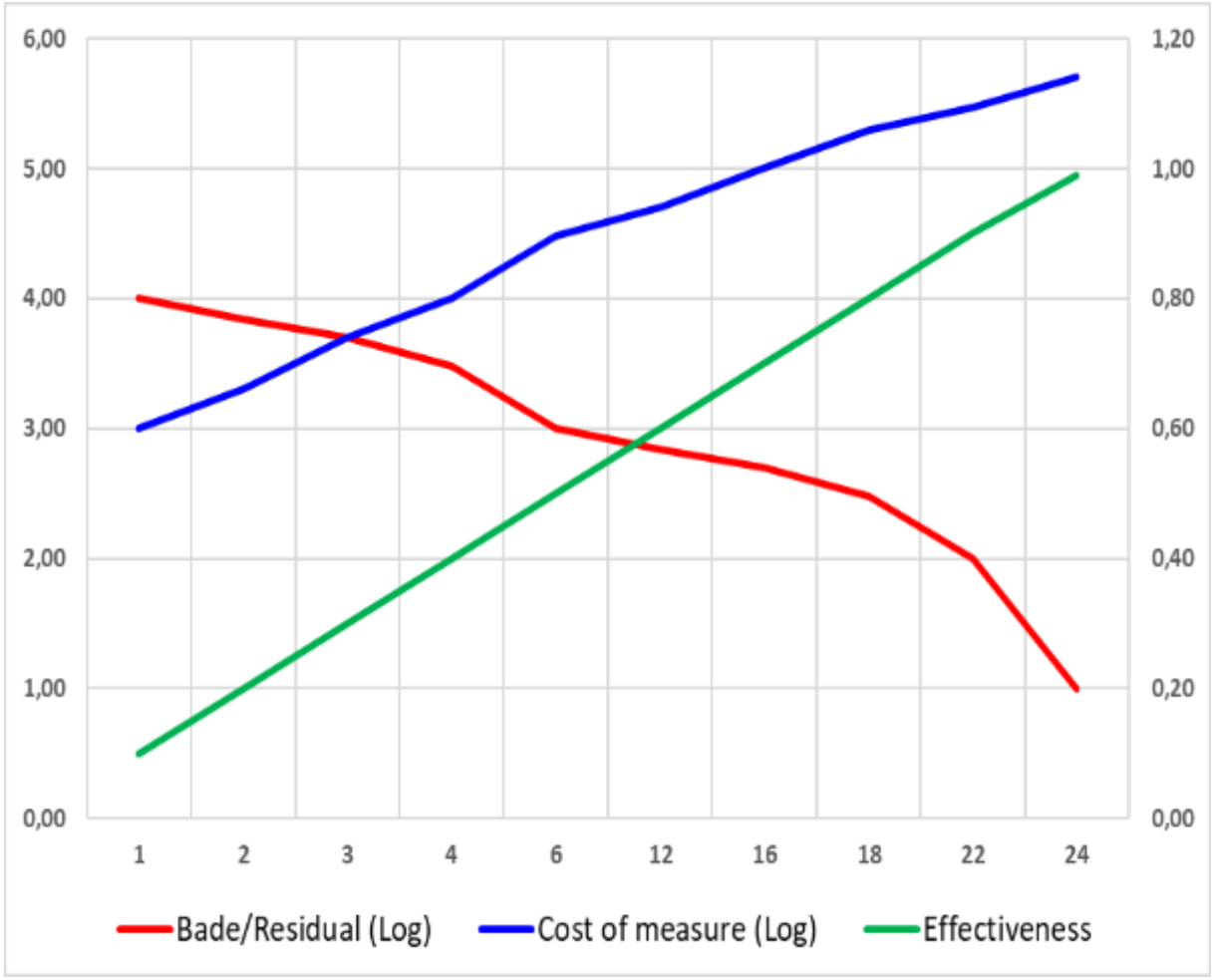
Parameter	Evaluation	Status	Consequence
X	Not considered	Fixed	-
R	Average opportunity	Dynamic	Average savings potential, as there is **minimal time** between identifying and "closing" a non-conformity
C	Average opportunity	Dynamic	Average savings potential, as fewer auditors with even workloads are required due to the optimal frequency of audits
F	A significant opportunity	Dynamic	Significant savings potential, as the **reduction of residual risks** occurs faster due to the increased frequency of audits
Y	A significant opportunity	Dynamic	Significant savings potential, as some critical incidents at CII facilities can be closed faster and **without penalties from regulators** due to the increased frequency of audits

5. The assessment of the effectiveness of the ISMS

$$К_{ISMS} = \frac{\frac{I_{curr}}{I_{base}} \sum_{i=1}^{m} \sum_{r=1}^{3} ISMS_{measure\ i} \cdot \alpha_{ir}}{\sum_{j=1}^{n} A_j V_j}$$

I_{curr} – the number of identified IS incidents for the current period;
I_{base} – the number of IT-Security incidents for the previous period;
i (1, m) – the list of protection measures;
r (1, 3) – the types of audit (**first, second and third party**);
$ISMS_{measure\ i}$ – the cost of the *i*-protection measure;
α_{ir} – **the assessment of the effectiveness** of the *i*-protection measure based on the results of the *r*-audit;
j (1, n) – the list of protected assets;
A_j – the cost of the protected asset (CII object);
V_j – the assessment of the significance of the protected asset (CII object).

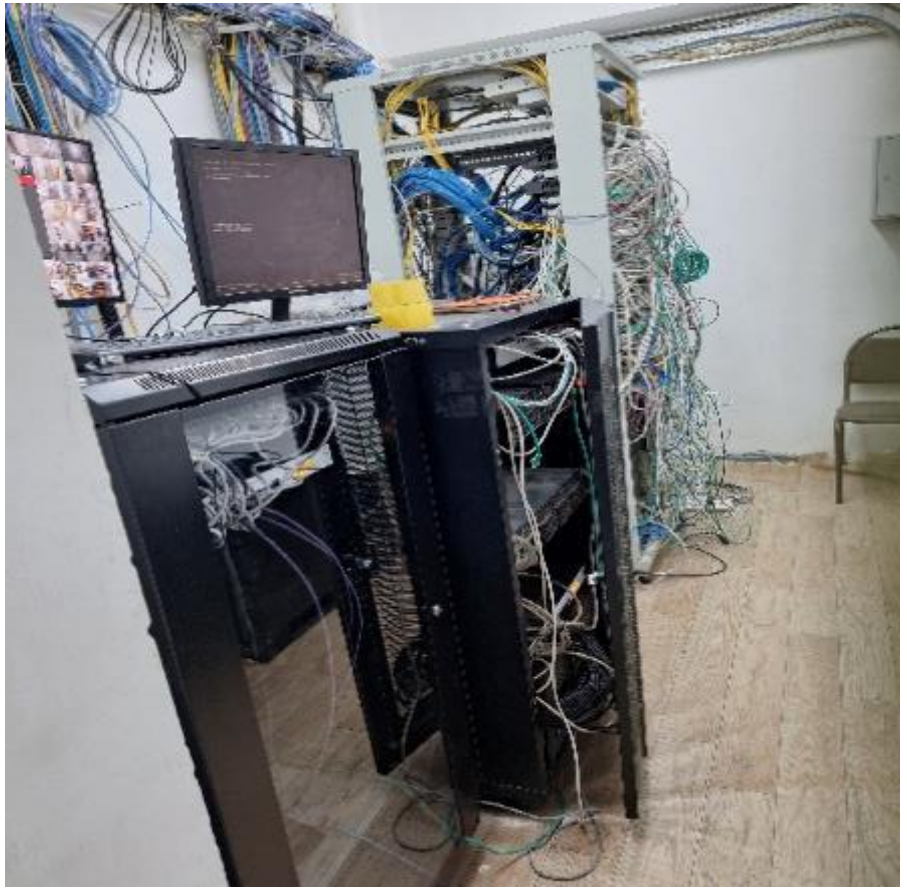
5. The assessment of the effectiveness of the ISMS



Ratio of residual and baseline risks to the cost of protection measures and the number of audits

As can be seen from this example, it is optimal to conduct three audits per year for a specific CII facility, which will reduce the residual risk to the base-line by a factor of 5,000 (determined by the ratio of the number of security incidents before and after the audits), at a cost of approximately $5,000 (ensuring an equal logarithmic function value of approximately 3.7 for two variables).

6. The assessment of the effectiveness of the ISMS. Example



Server room after the 1st IT-Security audit



Server room after the 2nd IT-Security audit

7. Conclusion

The presented work discusses theoretical and practical issues for solving the problem of ensuring a specified level of safety of CII facilities while reducing the cost of conducting management system audits.

It is proposed to perform management system audits not based on the formal requirements of a "fixed" annual audit, but with a frequency determined by production needs, the presence of non-conformities, and the maturity of the risk management system.

The proposed method of conducting operational audits ensures a reduction in cost, time, and residual risks for companies involved in the implementation of oil and gas projects.

Ensuring Operational Audit Of Critical Information Infrastructure Management Systems

Thank you!

Livshitz Ilya
ITMO University, IT-Security faculty, Russia

+7 (921) 934-48-46
Livshitz.il@yandex.ru