

**Business case for an**

**Information Security Management System (ISMS) in *HP Banking* based on the ISO/IEC 27000 series standards (ISO27k)**

**Executive summary**

|  |  |
| --- | --- |
|  | **Benefits** |
| • | As a result of ISO/IEC 27001 certification, HP Banking claims a number of benefits, including better security for the firm and its clients, assurance of best practices to new and existing clients, increased security awareness among personnel, and improved security documentation and reporting. |
| • | At HP Banking, security is now a top priority for the company's board of directors, which has led to operational buy-in and financial support, and has made security an important element of the outsourced business.  **Costs** |
| • | The certification cost section illustrates how various cost sources may become savings sources by decreasing budget requirements based on the implementation option selected. |
| • | All effort spent to meet a project deadline and users’ needs may be useless if cost overruns exceed the added value makes a budget in a project a critical component to facilitate value creation and preservation. |

# Introduction, scope and purpose

International clients know HP Banking (PVT) Ltd. as a leader in international customer data. Among its clients' extremely secret and sensitive

information are extensive databases of customer names, addresses, emails, phone numbers and other important metadata, according to the business. Securing global consumer information requires the collection, cleaning up, analysis, and prioritization described above, as well as the integration of different data silos from multiple sources.

Companies in retail, consumer electronics, marketing and publishing are among the company's clients. HP Banking is set to expand its team of specialists and focus on clients that are seeking for comprehensive, customizable, and secure MDM solutions that will help them deliver the best possible experience to their own consumers, thanks to its ISO/IEC 27001 Information Security accreditation.

# ISMS benefits

As a result of ISO/IEC 27001 certification, HP Banking claims a number of benefits, including better security for the firm and its clients, assurance of best practice to prospective and current clients, increased security awareness among personnel, and improved security documentation and reporting.

## Information security risk reduction

• For HP Banking wants to succeed, security requirements are a need. In addition to financial and technology firms, cyber thieves are now targeting other types of companies. They pose a danger to every firm in the world. This is due to the fact that high-profile security breaches are becoming increasingly common. However, this is only the first of many steps. External assaults are common, and their financial costs are substantial. **–**

## Implement a security policy

* Also, there are additional variables that might pose a cyber danger to a company. As a result, they are less technologically sophisticated. HP Banking’s information security defenses are affected by the human aspect. More senior persons are less likely to become malevolent insiders. Employees in the lower levels of the organization are the ones that have the most influence on security. Assign and monitor their access levels with a keen eye. As determined by malevolent insiders, the most common source of data loss is privilege misuse. **– Strengthen the Carbon Life Form**
* HP Banking have established a "Bring Your Own Device" policy in order to provide your employees with better working conditions and a more flexible work environment. The good news is that BYOD rules are becoming more widely known. On mobile devices, password security is still the preferred method of protection. **– BYOD Policy**
* An attack on security requires a well-thought-out strategy. What can be done to avoid a cyber assault, as well as what can be done in the case of one? As a result, HP Banking is prepared to handle these situations: **– Recovery Plan**

## Benefits of standardization

* Hardware and network equipment required by HP Banking are typically acquired from a single vendor or provider for each type of hardware and networking equipment. A reduced purchase cost, superior service and an overall increase in buying power are frequently the results. HP Banking Purchasing equipment in large volumes and from a select few vendors may allow you to negotiate better price and SLA conditions that meet your security and compliance needs. **– Reduced acquisition costs**
* When standardization is implemented in HP Banking, the decision-making process for technological investments and/or the acquisition of new hardware becomes less difficult. There are standards for the components of the IT infrastructure, so management and IT do not have to go through each item in great detail if the need arises. **– Simplified and collaborative decision making.**
* A technical analysis of the problem and issuing instructions can be carried out more effectively at HP Banking since everyone comes from the same platform. Thus, your workers will enjoy a more organized work environment, while technicians will have an easier time resolving network related difficulties. **– Efficient communications and resolution of issues.**
* In contrast, when standardized network infrastructure is used in the HP Banking company, IT management is simplified since most equipment functions in the same way. This makes it easy to solve many maintenance issues such as device updates, software patching, troubleshooting and other difficulties. **– Streamlined IT management.**
* 4 to 6 years from now, HP Banking might be seeking to update its data center. Due to the fact that as data gathering and business transactions continue to grow, their density and capacity needs will increase. Because of these possible IT resource shifts, it's a good idea to start planning for future infrastructure additions now. **– Qta rnldnmd sgd vqnmf vzx**

## Benefits of certification[[1]](#footnote-1)

* Security has been enhanced to safeguard clients' assets, resources, and people.
* Information security risks can be reduced by taking proactive steps, rather than waiting until a problem arises to fix it
* HP Banking want to be regarded as a reliable supplier and business partner who leads by example, has extensive information security credentials, and offers innovative solutions.
* Demonstrate that the HP Banking is highly qualified to pursue business with the world’s premier organizations
* Implement a comprehensive information security architecture that is well-established, proven, and constantly improved to decrease the risk of data breaches.

## Benefits of compliance

* However, while the return on investment from an ISMS might be substantial, the initial expenditure is usually triggered by external pressures such as HP Banking's most important customers There are too many hazards associated with cyber security and data breaches of any type to simply trust a handshake and a guarantee that a new provider would treat information properly. **– Gaining new consumers and retaining existing ones**
* Among the many aspects of ISMS, operational processes and duties are among the most critical. There are needs for change and capacity management, development, testing, and operational environments, malware controls, and information backup. **– Improving processes and strategies**
* Obligations relating to information security and any security requirements are to be avoided. In a good control, each information system and the organization's strategy to meeting all applicable legal, statutory, regulatory, and contractual obligations are recognized, recorded and maintained up to date in a clear and concise manner.**– Compliance with commercial, contractual and legal responsibilities**

# ISMS costs

## ISMS implementation project management costs

For the calculations of project management costs; Scalar assessment (Ed's version) has been used

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Factor** | **Weight** | **Scoring guide** | | | | **Your score** |
| **0%** | **33%** | **67%** | **100%** |
| **Executive, Board and senior**  **management support** | 15% | Senior managers are generally oblivious to or ignorant of the initiative. | Senior managers tolerate this initiative, on the whole. None are openly hostile anyway. | Senior managers are quite keen to see this project succeed. | Senior managers are positively insistent that the ISO27k ISMS implementation project goes ahead. . | 60% |
| **Strategic fit** | 14% | Both the ISMS and information security in general are diametrically opposed to the corporate ethos. | Information security has some strategic importance, but the ISMS itself is another story! . | Information security and the ISMS support strategic business objectives. | In the organization's strategy, information security is a key  component, with security and business objectives expressly connected | 35% |
| **Resourcing** | 14% | Simply finding someone suitable to complete this questionnaire has been a struggle. Good thing it's free! | The team is weak and the budget tight, but we'll manage, somehow ... hopefully. | According to this metric, the staff and budget are "enough" to "sufficient".  However, despite the obstacles that we face, we are able to accomplish our goals. | We've assembled a dream squad with an embarrassment-inducing amount of funding. There is "no problem" with the availability of resources. | 40% |
| **Quality of the**  **project team** | 11% | Nobody has actual ISMS implementation experience, and nobody is familiar with the ISO27k standards. | At best, it was mediocre. As a result, certain members of the  team claim to have knowledge and competence in this field. | Pretty good. Many within or consulting to the team either have direct personal experience of ISO27k ISMS implementations. | Excellent. The project manager/leader in particular has a great deal of real-world expertise in this field. | 70% |
| **Middle and junior**  **management support** | 8% | General managers are quite hostile to the initiative. | A few managers are supportive of the project but many are neutral and a few may be resistant or hostile. | Most managers either support the project or are neutral. | Middle managers are fully committed to the project. . | 75% |
| **True information security risk level**  **(currently)** | 7% | Absolutely out of this world. Given the severity/almost tangible nature of threats, vulnerabilities, and consequences, information security is a must-have, without a doubt | Tolerable to high. The corporate risk catalog contains a number of significant  information security threats, which are continuously evaluated and handled. | Medium to low. A few information security risks feature in the corporate risk catalog. | Very low or none at all, depending on the context. Organization's top twenty hazards include no information security or associated issues. . | 50% |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Blockers and culture** | 7% | There are several powerful people and things standing in the way of this project. It will be a miracle if it ever completes. T | There are going to be rocks on the road ahead but hopefully we can navigate around the worst of them. | There may be speed bumps ahead but we are not anticipating anything especially serious. | If anyone or anything even hints at becoming a problem, they will be dealt with, ruthlessly. | 40% |
| **Specialist support** | 7% | There is none: the ISMS implementation project team is all alone, out on a limb. | Some specialists might be persuaded to assist but most are reluctant. | Various specialists are already engaged with the project, and others could be persuaded to get involved. | Outstanding: security, risk, IT, compliance, governance, are either involved already or desperate to get involved. | 80% |
| **Breadth of scope** | 6% | Third parties such as suppliers and business partners are also covered by the ISMS. | A major component of the organization, such as all  operations in a specific nation  or locality, is covered by the  ISMS | Small numbers of departments or business units with good working  connections already in place are eligible to participate in the ISMS pilot program. | The ISMS is very tightly focused on a single, small unit, function,  department or business unit. | 30% |
| **Information security maturity**  **(currently)** | 5% | Prehistoric. The organization has almost no information security management processes in place | Basic. Some professionals are making the distinction between  IT and information security, but on the whole this project is  perceived as something within IT's domain. | Competent. Information security is being managed across much of the organization. | Cutting-edge technology.  Information security management is a field in which the company is always pushing the envelope. | 60% |
| **Compliance maturity** | 4% | The organization's compliance obligations relating to information security are simply not recognized as such | The organization appreciates that it has compliance  obligations but generally does the least amount possible. | The organization makes an effort to determine and fulfill of its information security-related compliance obligations. | As a result of regularly exceeding its duties, external compliance is a by-product of the organization's operations. . | 80% |
| **Scope definition** | 3% | Neither the ISMS nor the project scopes have been specified yet. | Some thought has been put into defining and drafting the  ISMS and project scopes | They are both well-documented, even though one or the other may not be entirely finished yet. | The scopes of both the ISMS and the project are | 85% |

Timescale estimate is given below.

|  |  |  |
| --- | --- | --- |
| **Timescale estimate** | **20.3** | Estimated months between approval of the ISMS implementation project and ISO/IEC 27001 certification |

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Project step** |  | **Estimated % of overall cost** |
| 1 | Obtain management support | 5% |  |
| 2 | Establish a project structure | 5% |  |
| 3 | Define the ISMS scope | 5% |  |
| 4 | Implement basic documentation for management system and risk  management | 10% |  |
| 5 | Perform risk assessment and risk treatment and develop mandatory documents | 10% |  |
| 6 | Implement all required controls | 20% |  |
| 7 | Perform training and awareness | 15% |  |
| 8 | Operate, monitor,  and evaluate the  ISMS | 20% |  |
| 9 | Improve the ISMS | 10% |  |
| 10 | Certify the ISMS |  |  |

## Certification costs

Considering the No. of People work in HP Banking company, counting the No. of days with minimum Audit time; as stipulated in ISO/IEC 27006:2015/AMD 1:2020, estimated certification cost is calculated.

|  |  |  |
| --- | --- | --- |
| **No. of people working** | **No. of days (Minimum audit time)** | **Estimated certification cost** |
| 876-1,175 | 13 | $23,400 |

# Conclusion

HP Banking's approach to customer service has been transformed by ISO/IEC 27001 accreditation. ISO/IEC 27001 has helped HP Banking decrease the risk of data breaches and standardize its operations in general. Consequently, workers have more consistency in their work procedures, and the company's resilience and service standards are increasing.

1. The ISMS may optionally be formally audited against and certified compliant with ISO/IERC 27001 by a certification body duly accredited by ISO. Normally management decides whether to go ahead with certification once the implementation project is finished and the ISMS is fully operational. [↑](#footnote-ref-1)