Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Continuous Improvement of Security Controls for Information Security

Anand Athavale

Independent Researcher
Decades of Industry experience in Data Management
andyathavale@gmail.com

Abstract

Monitoring various aspects of information security ranging from exposure, content and placements are only part of the necessary actions for information security. Improvement related to these aspects is just as important. Continuous improvement covers one-time actions and installing additional control mechanisms. These actions and additional controls depend on various aspects of the data itself and the interactions needed by the owners and users of that data on which the actions and controls are applied. Monitoring and capturing of exposure control cover long term aspects and are base level methods of information security. Continuous improvement aspects cover the time horizon aspect focusing on just-in-time approach provided by the advanced security control. These controls help in reducing the information risk greatly as described in this article.

Keywords: Proactive controls for information risk, Information risk management, Continuous improvement of risk posture

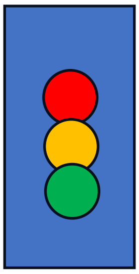
Introduction

Data exposure controls based on data type, content, location, and usage are base of managing information risk. However, the risk to data changes with time. These changes result from changes to data itself and changes to activity on data. Besides the change itself, the risk apatite is not consistent for all the data. Hence, just limiting exposure as remediation works for high-risk apatite data. It means if certain data has low risk even if got deleted or exfiltrated, it is not considered high risk. But certain data may have zero risk apatite, meaning, that data cannot leak or become available in any situation. For such data, additional control measures are required. It is important to note something which is not covered in this article. Here, the entire focus is to guard the data owned and stored by the organization. However, there are aspects of controls for data locations required to prevent misuse of open controls to use the data locations for storing tools use for data harm and theft.Those aspects are not covered here.

Risk Assessment

The data risk can be categorized into zero, low, medium, and high. There are many methods to assign risks based on various factors such as content type, implication of damage or leakage and so on. One of the methodsis to use the Traffic Light Protocol described Traffic Light Protocol 2.0 User Guide

[1]. The guide in fact is meant to facilitate effective collaboration of potentially sensitive information. However, the coloring definitions give an adoptable framework to categorize the data risk. In nut shell, these are the color coding for each information as defined by that document. To state explicitly, the aspects of trust within community as defined are not necessarily to be adopted. Recommendation is to use the document only to categorize risks based on the definitions. In other words, do not necessarily follow the controls mentioned in that document. Controls should be applied as listed in this article.



Traffic Light Protocol

i. RED - Information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved

ii. AMBER - Information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.

iii. GREEN - Information is useful to increase awareness within their wider community, but not via publicly accessible channels

iv. CLEAR - Information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release, shared without restriction

Three categories of continuous control improvements

Continuous improvement of controls related to data content and exposure can be categorized into three key areas, namely data placement or existence, data type and content and lastly change of exposure itself.

1. Data placement and existence:

   Data placement implies changing the data location to reduce risk. Again, here the focus is security and not the compliance. But, while moving the data to reduce risk, typically of type RED, compliance aspects of data sovereignty and data residency [2] need to be considered and met. Data placement improvements at minimum involves moving data to a location less accessible. For starters, it could be simply moving it to a location only accessible to CXOs or top-level management. This could also mean taking it down from a cloud or colocation facility [3] to a private and independently controlled data facility. It is important to consider that these actions to improve control are not necessarily mutually exclusive and sometimes can be taken in conjunction.It could also mean, shipping of that data to an isolated facility not accessible over network and then removing it from the current location. This movement to isolated location is mostly applicable to type RED data. The movement and removal depend on the accessibility required for that data to conduct business. This is where the monitoring aspect aid in decision making. If the data activity is already known for that data, impact of the movement and removal is already known. In addition to that, depending on the new location, which business users require the access post movement is also known minimizing disruption to business while reducing risk.

2. Data Type and Content

   Improvements in control to reduce information risk, typically for type GREEN and AMBER, one may start with simply changing the format. If there some data item you do not want to be changed easily, changing the format of data may help. As an example, you can covert a Word document into PDF to prevent any modification, while still allowing accessibility.

   More advance control examples include encryption. However, encrypting data entirely can become an issue for accessibility. But there are newer methods in structured data types, which allow for accessibility to remain relatively same while reducing risk with encryption. Oracle Transparent Data Encryption [4] is one such method.Another option is to anonymize data. Anonymization has two options. Pseudonymization, which means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified. Where a pseudonym is used, it is often possible to identify the data subject by analyzing the underlying or related data."Anonymization" option processes it with the aim of irreversibly preventing the identification of the individual to whom it relates [5].Datais consideredfully anonymized when it is not be possible to identify any individual identity in the anonymized data even with the aid of the original data. Which option to choosedepends on the risk level. RED type in the most cases should use anonymization. AMBER may use Pseudonymization.

3. Change of exposure

   Exposure change is one more method to improve risk posture. The simplest step in this is to ensure that no data, RED, AMBER or GREEN, should be exposed to everyone within the organization. If any non-CLEAR data is exposed to outside of organization on a permanent basis, that should also be immediately rectified. Depending on the content, notifications still may be needed to be issued in such scenarios.Besides these basic changes in exposure, here are more process and control driven methods of changing the exposure.

   i. Time driven

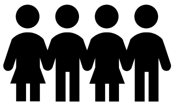
      Often the data applications offer a way to limit the access to the assignees for a specified time. A classic example of this is time-based expiring of access in SharePoint and OneDrive [6]. Similar features exist in several content sharing platforms. These can be used for both internal and external sharing.Linux has an option with autofs where, it only mounts a given share when that share is being accessed and unmounts it after a defined period of inactivity [7].

   ii. Dynamic Rule driven

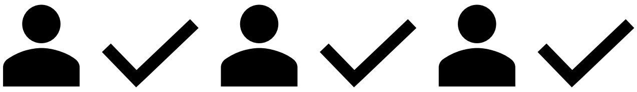
      Several data applications offer attribute-based control instead of static access assignments to groups or users. For instance, such applications allow you to define a rule-based access saying if the user’s attribute department=’Finance,’ then allow access to Finance data. Additionally, if there was a credential compromise for a non-finance user, financial data remains guarded unless the user can make a lateral movement to a finance user. This way, if a user transfers out of finance department to say, sales operations, the user automatically loses access thus improving exposure control.

iii. Multi-person Control driven

In Indian banking system, there is still a practice where a large amount operation, or critical operations require authorization from bank officers. Cashiers alone can not execute that transaction. Multi person controls are very similar. Here, the control allows to form a set of approving users to which a sensitive request initiated by someone outside of that set of users is sent.

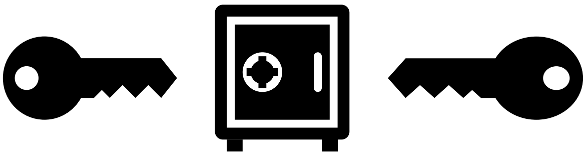


Set of Approving Users



Operation approval needs at least three persons to approve

These controls allow to define number of approvers that must approve the request to carry out such operation. Same controls can be installed where if extremely sensitive data (RED category) is being restored, the approvers first check who is restoring it, why and to where it is being restored and only then they would let the restore go through. Sometimes, this can get layered with another control which can best described by bank lockers. If you need to access your locker, typically, in secure locker rooms, you need your key and the supervising bank officer brings a bank key. Only when both keys are right, the locker unlocks. Similarly, some third-party vendors allow customers' data to be first encrypted by their key, and then, they also encrypt it with their own key.



Two keys needed to open the locker

This additional exposure control prevents data theft in case of exposure or leak of key from customer or vendor. This would mostly apply for backups of the RED type of data, which is needed for business and hence necessitates another copy to ensure recovery from any type of destruction. Some solutions also offer locking of data for a certain amount of time to prevent tampering or destruction. These are often referred as retention locks, data locks or WORM locks.

Challenges of exposure control mechanisms

i. Manual vs. automated

As explained at the beginning, the basis for applying improvement measures for information security depend on assigning accurate risk value to data. If done manually, it is prone to errors. Even if it is done automatically, post assignment of risk value, not all additional control steps are automated.That isthe first challenge.

ii. Democracy vs. training in data management

Data management is not necessarily restricted to IT admins. Shadow IT and individual projects often exist. Several times, not everyone is trained on tools and methods for applying additional controls. This too creates challenges of applying additional exposure controls.

iii. Acquisition and merger spawned heterogeneity

When multiple organizations merge or get acquired, often they are used to different data applications. Governing aspects for applying additional exposure control methods often take a long time, or, sometimes that never happens. This, additional exposure controls get applied to only partial data estate.

iv. Cost Efficiency vs. security

The challenge of having to choose between cost efficiency vs. additional control measures mainly applies to data locking or immutability controls. A very few data management solution have ability to do granular locking. For those solutions lacking efficient granular locking, end up locking large amount of data for much longer than needed. This increases the costs of additional controls like data locking or WORM locking.

Conclusion

Monitoring and observing techniques are only part of the measures for information security. Based on the criticality and impact of data destruction, or, theft, risk levels increase and additional measures are required. Additional measures range from relocation, obfuscation to locking against destruction and tampering. Allowing exposure to remain on need-to-know basis is only the start. But ensuring continuous adjustments to the access ensures the access being available only for required duration reducing the risk further. Instead of relying on forever granted permissions, seeking approval when access is required for most critical data ensures constant check and prevents against a single credential compromise leading to information security being compromised. However, while putting those additional controls in practice, the challenges associated with those also need to be considered.

References

[1] Cybersecurity and Infrastructure Security Agency, Traffic Light Protocol 2.0 User Guide (September 2022), https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf, (June, 2023)

[2] Alex Tuck, Data Centre Magazines, Data residency and data sovereignty: what's the difference?, (July2022), https://datacentremagazine.com/articles/why-its-important-to-know-where-your-data-is-stored, (July, 2023)

[3] N/A, Strategic Guide To Data Center Colocation, (2022), https://www.tierpoint.com/it-strategic-guides/colocation-data-center/, (June, 2023)

[4] Ruhi Sharma, Oracle Database Administrator, Racskspace Technology, Transparent Data Encryption (November2022) https://www.rackspace.com/blog/transparent-data-encryption, (June2023)

[5] Data Protection Commission, Guidance on Anonymisation and Pseudonymisation (April 2022), https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf, [June 2023]

[6] Gregory Zelfond, SharePoint Consultant, How to set up expiration for guest access to SharePoint and OneDrive (February 2022) https://sharepointmaven.com/how-to-set-up-expiration-for-guest-access-to-sharepoint-and-onedrive/, (June2023)

[7] Tyler Carrigan, Red Hat Blog, Mount NFS filesystems with autofs (August2020) https://www.redhat.com/en/blog/mount-nfs-filesystems-autofs, (June2023)