MyCorporate Acquisition Security Standards

2016

# Document Control

## Document Version and Revision History

The following document version control section documents the changes made to the document. The Nature of the Change section will identify areas that were modified within the document and briefly describe the changes made. Minor versions are used when small changes to the document such as spelling or grammatical errors are updated. A minor version is applicable as long as the intent of the section does not change. Major versions will need to be used when sections of the document or removed or completely changed. Be sure when updating the document version that the version in the header section of the document is updated to coincide with the current version number.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Nature of Change |
| 14.10.2015 | 1.0 | John Doe | First Version |
| 19.11.2015 | 2.0 | Lena Strict | Rewriting |
| 22.11.2015 | 2.1 | Marianne Sicherheit | Minor modifications |
| 26.01.2016 | 2.2 | Lena Strict | “Connect” and “Combine” phases added, corrections to Integration Plan and “Capture” phase, IT Security Team role paragraph |

## Approval

|  |  |  |
| --- | --- | --- |
| Role/Job Title | Name | Approval Date |
| CISO | Marianne Sicherheit | 22.11.2015 |
| CISO | Marianne Sicherheit |  |
|  |  |  |
|  |  |  |

# Table of Contents

[1 Document Control 1](#_Toc486368113)

[1.1 Document Version and Revision History 1](#_Toc486368114)

[1.2 Approval 1](#_Toc486368115)

[2 Table of Contents 2](#_Toc486368116)

[3 Overview 3](#_Toc486368117)

[4 Intended Audience 3](#_Toc486368118)

[5 Purpose 3](#_Toc486368119)

[6 Scope 3](#_Toc486368120)

[7 Definitions, Acronyms and Abbreviations 3](#_Toc486368121)

[8 Integration 4](#_Toc486368122)

[8.1 General considerations 4](#_Toc486368123)

[8.2 IT Security Team role 4](#_Toc486368124)

[8.3 Integration Models 4](#_Toc486368125)

[8.4 Integration Process 5](#_Toc486368126)

[8.5 Integration Plan 5](#_Toc486368127)

[8.5.1 Capture 5](#_Toc486368128)

[8.5.2 Connect 5](#_Toc486368129)

[8.5.3 Combine 6](#_Toc486368130)

[8.5.4 Consolidate 6](#_Toc486368131)

[9 Integration Steps 0](#_Toc486368132)

[9.1 Capture 0](#_Toc486368133)

[9.2 Connect 0](#_Toc486368134)

[9.3 Combine 0](#_Toc486368135)

[10 Policy Compliance 1](#_Toc486368136)

[10.1 Exemption 1](#_Toc486368137)

[10.2 Non-Compliance 1](#_Toc486368138)

[11 Related Standards, Policies and Processes 1](#_Toc486368139)

# Overview

The process of integrating a newly acquired company (“Target” company) by MyCorporate can have a drastic impact on the security posture of both. Activities that can have an impact are the followings:

* the acquisition model;
* IT integration processes and organizational structure;
* business processes and activities;
* business continuity issues;
* the size and complexity of the company to be acquired;
* privacy, regulation and compliance – both on IT and non-IT

The network and security infrastructure of the two merging entities may vary greatly, as well as the workforce may have a drastically different culture and risk appetite.

# Intended Audience

This document is intended to be read, approved and used by individuals with the “need-to-know” only.

* IT leadership at MyCorporate and Target
* ITSEC team
* M&A/Integration team involved in the assessment of the new acquisition

# Purpose

The purpose of this policy is to establish the IT Security team responsibilities regarding corporate acquisitions, and define the minimum security requirements of an IT Security acquisition assessment.

# Scope

This document applies to all target companies acquired by MyCorporate, and pertains to all real estate, systems, networks, equipment, hardware, software and firmware, owned and/or operated by the acquired company.

# Definitions, Acronyms and Abbreviations

| **Acronyms** | **Meaning** |
| --- | --- |
| ITSEC | IT Security Team, direct and dotted line reporting to the MyCorporate CISO |
| Target | Company to be acquired by MyCorporate |
| ATEAM | Acquisition Team from MyCorporate, which includes ITSEC representatives |

# Integration

## General considerations

Acquisition assessments are conducted to ensure that there is clear understanding of the security risks and required investments/improvements that the Target being acquired by MyCorporate will pose. This includes corporate networks, internal systems, Cloud infrastructure, and the management of confidential/sensitive information.

ITSEC will provide personnel to serve as active members of the ATEAM throughout the acquisition process.

## IT Security Team role

The ITSEC role is to assess and evaluate information security risk, establish the minimum, non-negotiable IT Security topics that needs to be established, and develop an IT Security integration plan along with the rest of IT. The plan will work with the Target IT team to implement solutions for any identified security risks and to align the IT Security posture.

## Integration Models

The integration will follow a model which depends on the size, location and other strategic considerations.

| **Target Characteristics** | **Security Guidelines** | **SLAs** |
| --- | --- | --- |
| **SMALL**   * Small employee base (< 200 employees) * Low complexity * Private ownership * Little to no geographical diversity * No separate legal entities * No/limited need to keep the same facilities * No/limited to keep the existing technologies * Purchased for limited product portfolio, technology, talent, or local presence | * Baseline security controls Target is fully absorbed into MyCorporate IT infrastructure * All IT labor is absorbed into IT global business units | * Security controls established or confirmed in less than 100 days |
| **Medium**   * Similar to previous kind, but Target has certain identifiable complexities that require specific sensitivity during integration * Fewer than 500 employees * Needs to be stand-alone for a certain period of time * During stand-alone time, Target maintains defined non-compliances * Supports its own IT infrastructure during the stand-alone phase | * Integration of Target may be full, hybrid, or standalone * All IT labor is absorbed into IT global business units | * Operation integration of some IT infrastructure may take +180 days * Processes may take 3 to 9 months |
| **Large**   * More than 500 employees * Relatively large operations * Significant multinational presence and subsidiaries * Target contains certain identifiable complexities that require specific sensitivity during integration | * Integration of Target may be full, hybrid, or standalone * IT labor can stay funded by Target company | * Operation integration of some IT infrastructure may take +180 days * Customized integration plan * IT Support is shared * Processes take more than 12 months |

## Integration Process

The integration process follows the depicted steps:

* Assess and evaluate the Target posture, policies, standards, guidelines, and risks, including physical threats;
* Identify possible gaps and increased security risks;
* Develop an **Integration Plan** with precise milestones for closing the gaps between current and desired end state;
* Finalize integration: agreed-upon designs are implemented, and operation is turned to standard support.

## Integration Plan

The ITSEC team has to review the Integration Plan to assess it is following best practices for IT Security, propose corrections where necessary and veto proposals which are deemed unacceptably insecure.

The integration plan follows the four Cs processes:

* Capture
* Connect
* Combine
* Consolidate

### Capture

This process is ubiquitous to all deals, regardless of the deal type or the model used for integration. During the capture process, ITSEC collects information on assets, people, budget, and strategy from both internal MyCorporate functions and the Target to evaluate security and risk profile.

Internally, information on the strategic intent of the deal is provided to the ATEAM. Other information includes facilities disposition, product plans, and organizational plans; this information aids in overall security planning.

### Connect

Connect establish connectivity for the initial core infrastructure, setting up primary communication and collaboration tools and systems. This stage typically involves an interim step of creating a VPN tunnel, followed as quickly as reasonable by LAN/WAN interconnection, and then integration of other core IT infrastructure services.

The connectivity can follow different steps, depending on the complexity and size of Target. The focus is on immediate connectivity, followed

### Combine

Integrate business systems and processes.

### Consolidate

Realize economies of scale through organizational asset consolidation.

# Integration Steps

## Capture

As mentioned, in this phase information from the Target are captured.

This phase –at least, at the beginning– is happening under a “need to know” restriction; it is important to be aware of this. Information security takes precedence over information completeness.

This information is retrieved by questionnaire and/or interviews. The desired deliverable is a thorough and accurate security site survey.

Questionnaires can be built directly from this list. At each step, the ITSEC team seeks to assess possible risks, and define the minimum security standards acceptable, based on the level of risk and risk appetite.

It is mandatory, that the technical integration between Target and MyCorporate cannot happen before a physical inspection and a site survey are performed, to clear up for possible physical security risks (as for points 12 and 13). Inspection can be pursued by ITSEC or representatives delegated by the ITSEC team.

| **Step** | **Domain** | **Verification** | **How-to** | **Objectives** | **Minimum Acceptable Level** |
| --- | --- | --- | --- | --- | --- |
|  | Digital Identities | Verify status of identities in main identity store (use of unique IDs, generic accounts, password policy, Groups’ usage, GPOs, Federations, etc.).  Verify if anything is outside of the main identity store (e.g. VPN accounts, Cloud accounts, supplier accounts, etc.). | * Interview with IT admins from Target. * Snapshot of information from AD/LDAP. * Interview with business units which manage other tools (Cloud etc.), to understand how this is managed | * Ensure appropriate controls are in place to protect Target environment and data * Get an idea of the complexity of the DI structure of the Target. * Understand usage of Cloud applications and identities. * Understand how restriction of access to information happens in Target. | * There is a Directory Service * Unique IDs are used * Permissions are assigned via Groups in the Directory Service * Service and Cloud accounts are gathered, minimized, and under control * Sensitive files are shared in a secure way |
|  | Admin Accounts | Verify status of admin account management in main identity store, if managed there.  Verify if anything is outside of the main identity store (e.g. VPN accounts, Cloud accounts, supplier accounts, etc.) | * Interview with IT admins from Target. * Snapshot of information from AD/LDAP and other tools. | * Ensure admin account controls are defined, implemented and reviewed to protect systems and data * Understand how IT administrative actions are performed, what the procedures and practices are, and who has the ownership and responsibility. | * Admin accounts are managed under a Directory Service * Admin accounts are unique for each admin * Central ownership of who gets appropriate rights * Process for removing rights as appropriate |
|  | Endpoints / Client Systems | Verify how workstations and clients are managed.  Verify which level of security is applied, especially concerning:   * Disk encryption and other data leakage prevention measures – including on mobile devices * Remote Access/VPN * Patch management * AV/malware control * Vulnerability management * Secure disposal procedures for clients * Software procurement and installation procedures * 2FA, if present * Network Access Controls   Understand how Printing is setup and secured. | * Interview with IT admins from Target. * Snapshot of information from AD GPOs, as well as other tools’ management interfaces (e.g. SCCM, AV console, etc.) if present. * Understand if there are different classes of users, which may get different kind of clients or have more rights. | * Ensure policy, processes and capabilities and tools are in place to protect Target environments and data. * Understand how the client environment is managed and identify critical risks. * Note: Consider secure printing and hardware disposal procedures | * Client types are reduced as much as possible * Clients use a supported Operative System * Users have restricted access to admin accounts on clients * Disk encryption is applied, especially for mobile systems * Security patches on clients are applied at least monthly * There is a procedure to update software at least quarterly, or after major releases * AV from a reputable vendor is installed, and signatures are updated at least daily * A secure procedure is defined for software updates and new software rollout * A client disposal process is in place * A protection for threats coming from emails is in place * Awareness against phishing is performed * An adequate restriction (by means of technical access control, physical access restriction, or procedural) on allowing access to the Office Network only to authorized devices and people, is in place * Precautions are in place for company devices brought on business trips |
|  | Servers | How servers are managed.  Verify which level of security is applied, especially concerning:   * Disk encryption and other data leakage prevention measures * Patch and version management * AV/malware control * Vulnerability management * Virtualization * Secure disposal procedures * Software procurement and installation procedures * 2FA if present * PAM/PIM tools, if present * Physical access restrictions | * Interview with IT admins from Target * Snapshot of information from AD GPOs, as well as other tools’ management interfaces * Understand if there are different classes of users, which may get different kind of clients or have more rights * Understand where “crown jewels” are located, and which are Tier-1 and Critical systems | * Ensure policy, processes and capabilities and tools are in place to protect Target environments and data. * Get a picture of how server and infrastructure are managed and what the most important risks are * Understand if there are criticalities about | * Minimum level of physical restriction are applied to server access * There are some forms of malware mitigation in place on servers, such as an AV from a reputable vendor; signatures are updated at least daily * Software installation and updates must have a secure procedure * Security patches on servers are applied at least quarterly * There are central repositories for rules, security controls and priorities * Some form of hardening is applied for servers which host critical assets |
|  | Networks | Internet Outbreak  Internet Presence  VPN  MPLS  Voice Networks  Admin/Management Networks  Office LAN  NAC (If appropriate)  Internal networks segmentation | * Interview with IT or network admins from Target * Network and data-flow diagrams * Understand where “crown jewels” are located * Define required standards for target based on risk and need | * Protect Target from security risks, while also protecting MyCorporate’s environment from new risk resulting from networks’ integration * Protect Target’s critical assets through network security best practices | * Secure connectivity between MyCorporate and Target * Secure access from Target staff and stakeholders * Redundant/resilient connections to the Internet are in place * Periodic security controls review for compliance * At least some form of network segmentation and/or filtering segregates critical assets |
|  | Hosting | External / Internal Hosting  Cloud Presence  Website(s) | * Inventory all hosting activities * Evaluate security capabilities of hosting vendors * Understand contractual and security controls with partners * Review Target policies for cloud usage | * Understand hosting risks and ensure appropriate controls are in place * Mitigate hosting risks if necessary | Minimal controls include:   * contract controls * confirmation of hosting partners security controls * policies for Target hosting and cloud usage * security controls to protect / encrypt co-hosted data |
|  | Email | E-Mail System  E-Mail Servers  E-Mail Backbone, Relay, MX  Anti-Spam, Anti-Phishing | * Understand email infrastructure and risks * Confirm email protection tools are in place and proactively managed | * Ensure Target has appropriate anti-phishing, malware and anti-spam tools in place. * Protect MyCorporate environment from Target email risks | * Email use policy in place * User awareness for email security and anti-phishing * Tools and processes for anti-phishing, malware and anti-spam |
|  | Data Recovery | Data Recovery Capabilities  Backup  Redundancy  Disaster Recovery  Test of backup media  Restore test  Rehearsal of DR | * Understand data backup and recovery tools, processes, capabilities and risks * Review backup / restore testing evidence * Review DR plan | * Ensure Target has adequate backup/recovery processes, tools and capabilities * ID opportunity to leverage MyCorporate capabilities * Understand DR capabilities and risks | * Proven data backup / recovery capabilities * Testing of solutions * Viable DR plan |
|  | Boundary Defenses | Firewalls  Next-Generation Firewalls Proxies  URL filtering  VPN concentrators  Site-to-Site VPNs  Use of encryption  Web Application Firewalls  DoS/DDoS protection | * Interview with IT or network admins from Target. * Review of security architecture * Ensure appropriate tools, processes and capabilities are in place * Review standards / process documentation | * Ensure that Target has an adequately architected, managed and tested environment to protect data and systems, and MyCorporate after integration | * Reputable brands and management of Firewalls are in place * Reputable brand of URL filtering/proxies, filtering from threats coming from web browsing, are in place * VPNs are used for B2B communication and remote access of users * Adequate encryption in transit and/or at rest is in place for business applications * Web services are adequately protected |
|  | Inventory | Inventory of clients, servers, hardware, software  Reconciliation procedures  Configuration management tools  Network diagrams and plans | * Review inventory and associated documents * Perform spot checks to ensure it is up to date and managed | * Ensure Target has managed inventory, CMDB, network plans | * Full asset inventory * Network diagrams |
|  | Operational Security | Pre-hiring procedures for admins  Periodic verification of access rights  Syslogs / audit loggings  Monitoring of third party and remote access  Strong/multi-factor authentication  Regular vulnerability assessment  Regular penetration tests  Management of keys and certificates  Tools for data encryption/data masking  Incident Management procedures  External Security Service reviews (compliance, certification, quality) | * Review of new-hire process documentation to ensure controls are in place for background check, role definition and process for enforcement of work quality * Review evidence of logs, access rights and separation of duties * Review recent pen test results or conduct pen test * Review key management process documents and test evidence process is followed * Confirm encryption is functional and followed fully * Review incident response plan and evidence of periodic updates * Review External security service reviews | * Ensure Target has operational security processes and tools in place, and that they are tested to ensure compliance * Confirm Target has staff with security skills and focus, and is responsible for data and system protection | * A hiring processes is in place * Log management and review is in place * Monitoring processes and capabilities are in place * Multi-Factor authentication is used for key systems and remote access * Periodic vulnerability assessments and pen tests are conducted * Process for mitigating critical findings is in place * Encryption of mobile systems and sensitive data is in place * Tested and periodically updated incident response plan is in place |
|  | Physical | Physical Security plan  Access control systems  Critical/High Impact IT infrastructure is physically segregated  Physical access is logged/monitored | * Review physical security plans, tests and reviews * Test physical security controls | * Ensure physical controls exist and are managed | * Physical Security plan * Access control systems * Critical/High Impact IT infrastructure is physically segregated * Physical access is logged/monitored |
|  | Wireless | Wireless segregated from Critical/High Impact IT infrastructure  Wi-Fi corporate and guest  Wi-Fi monitoring  Wi-Fi access control | * Review wireless security policies, standards and processes * Review wireless testing documents * On-site or delegated site surveys | * Ensure Wireless environment is secure, managed and periodically tested to avoid data loss and intrusions | * Wireless segregated from Critical/High Impact IT infrastructure * Corporate and guest networks are separated * Wi-Fi monitoring and access control are in place * Site perimeter is monitored |

## Connect

This phase of the acquisition is probably already happening “in clear sight”, that is, the basic risk assessment has been performed and the acquisition is public news. In this phase, information completeness is paramount.

After this first assessment is complete, through an evaluation of the existing environment the ATEAM will have to propose an **Integration Plan**. The integration plan requires specific budgeting for the necessary infrastructure services to be integrated or replaced, as well as business processes and systems, and timing.

The Integration Plan includes three sections:

* **Technical integration**: this includes LAN/WAN, voice, client computing, PC hardware, productivity applications, data centers and hosting, engineering tools, backup solution, printing, video and telephony, and other infrastructure services.
* **Business processes and systems**: evaluate existing business processes and systems, working with business owners to identify process changes and facilitate process and system changes to enable business functions. Business functions include IT support for hardware and software, engineering, manufacturing, HR including new hires and leavers’ processes, sales, manufacturing, internal and external web, finance, customer services, business-to-business and suppliers management, and so on.
* **Timing**: negotiate for agreement on the overall plan and timing, aiming for an overall agreement between all affected parties must be reached on how and when the Integration Plan will be implemented. Primary stakeholders include MyCorporate, Target and ATEAM members and/or virtual teams involved in the acquisition.

The Integration Plan must also negotiate from an “as-is” to a “to-be” state for Target.

## Combine

In this phase, resources, staffing, processes, and systems of Target are combined with the ones from MyCorporate. Business processes are as much as possible leveled, and IT tools are unified. Target has assumed a comparable or the same security posture as MyCorporate. Differences in processes and IT Security posture, as well as “misses” from the Integration Plan, are documented and signed off by key stakeholders (leadership, executives, CISO).

The agreed-upon designs are implemented, and operations – including ITSEC – are turned over to standard support.

Weekly or recurring meetings can be setup to assess integration phases are carried out by the ATEAM as expected, and do follow IT Security best practices.

# Policy Compliance

The ITSEC team will verify compliance to security policies through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from the policy owners.

## Exemption

The time required to have Target fulfill both the Minimum Acceptable Levels of Security and to standardize to MyCorporate standards are depicted in the Integration Plan.

In the event that milestones in the Integration Plan could not be met, the MyCorporate Chief Information Security Officer (CISO) must acknowledge and approve an exemption, or suggest short term mitigation controls.

Exemptions are always time-constrained and must indicate the time required to recover compliance.

## Non-Compliance

Non-compliance to the Integration Plan must be escalated to the Project Manager of the ATEAM.

In the case that specific MyCorporate policy violations are detected, the responsible person will be subject to the disciplinary action provided by MyCorporate policies.

# Related Standards, Policies and Processes

If the company processes and/or stores Personal Identifiable information (PII) or Personal Health Information (PHI) they will be required to adhere to MyCorporate’s Data classification standards and the privacy laws where the data subject lives.

If the company develops software/hardware for the medical industry they will be required to follow MyCorporate’s secure development practices.