Revista de Comptabilitat i Direcció
Vol. 34 any 2022, pp. 125-137

El paper de les tecnologies de la informació en el procés de *Due Diligence*

IVAN CASTELLTORT
Universitat Rovira i Virgili

Data de recepció: 30/01/2022
Data d'acceptació: 26/02/2022

RESUM

És inevitable que la Tecnologia de la Informació o IT tingui un paper rellevant avui dia en el funcionament de qualsevol empresa. Inevitable també que qualsevol procés de *Due Diligence* hagi de considerar la tecnologia de l'empresa que avalua com un factor que pot alterar el resultat final de la inversió necessària per a la compra.

De totes les operatives que la IT representa avui en la majoria de les empreses, destacarem aquelles que poden ser més rellevants per a la *Due Diligence*. Començant per les persones que conformen el departament d'IT amb els seus rols i talents, per a seguir amb els aspectes que poden impactar reputacionalment si no es tenen com una política de seguretat tecnològica que blindi en la mesura que sigui possible contra ciberatacs o una infraestructura que permeti la continuïtat del negoci sobre la base d'uns excel·lents nivells de servei i arquitectura redundada en punts clau dels sistemes. Aquests punts i alguns més són objecte de la primera part de l'article.

A la segona part comentarem sobre les oportunitats que les diferents aplicacions comercials disponibles en el mercat poden oferir per a reduir l'esforç necessari per a completar un procés de Due Diligence.

I acabem oferint una sèrie de conclusions relatives al paper de la IT en el procés de *Due Diligence*.

Classificació JEL: G34, K42, H25, M14, M40.

PARAULES CLAU

IT (Tecnologia de la Informació), Ciberseguretat, Pla i Mapa de Sistemes, Virtual *Data Rooms*.

ABSTRACT

There is no chance to find a company where Information Technology is not relevant for the core business operations. For this reason, there is no way for a *Due Diligence* Process cannot consider what IT is supplying to the business health and future. On the other hand, IT has its own impact in what could be the final figures of the investment required to purchase.

Among a vast number of operational procedures which IT implements in most of the modern companies, we will highlight a bunch of outstanding ones. Beginning with the IT people IT and their talents and moving on to a set of policies that will assure a good protection against cyberattacks and a reliable platform able to provide the required business continuity with no lacks of IT architecture redundancy. We will cover this in the first two chapters of the article.

Chapters three will discuss about some opportunities to make *Due Diligence* process easier to run. In particular, we will have a look to some tools which can be deployed to handle in a more efficient way the data and procedures required for a right development of the *Due Diligence* process.

Last but not least, we will be settling what should be the paramount points no one can miss when talking about the role of IT in the *Due Diligence* process.

JEL classification: G34, K42, H25, M14, M40.

KEYWORDS

IT (Information Technology), Cybersecurity, Systems Plan and Map of IT Services, Virtual Data Rooms.

1. IT en el procés de *Due Diligence*

El procés de *Due Diligence*, en la seva funció de recerca de les diferents àrees de negoci de l'empresa a valorar ha de tenir molt en compte aquells aspectes tecnològics que puguin generar uns riscos o significar sinergies en el càlcul final de la inversió necessària per a l'operació. En el món de l'empresa actual, la dependència de la tecnologia de la informació o IT, d'ara endavant, sol ser rellevant. La majoria de les empreses donen suport a les seves operacions diàries en un component tecnològic que s'ha anat complicant després de la irrupció d'Internet fa ja més de vint anys.

Hi ha diversos aspectes tecnològics clau que un rigorós procés de *Due Diligence* ha d'analitzar per a valorar després potencials impactes. L'objectiu d'aquest article en aquest punt no és ser exhaustiu sinó més aviat aportar al lector una perspectiva d'allò que pot ser important amb un llenguatge que tracta de fugir del tecnicisme habitual de molts textos. Aquests aspectes s'enumeren en els següents apartats de forma classificada i seqüencial sense que l'ordre impliqui una escala de major a menor risc o impacte.

Existeixen al llarg de tot el text diversos esments a aspectes particulars d'empreses purament tecnològiques. Ens referim a empreses de serveis o productes informàtics o també a les famoses *start up*s tecnològiques. És evident que aquesta categoria d'empreses incorpora característiques IT que empreses d'altres sectors no requereixen en la mateixa mesura. Per a major claredat per al lector, aquests esments són sempre referenciades en el text de tal manera que no donin lloc a cap confusió.

Finalment, ens ha semblat interessant incorporar al text un apartat independent on es comenta breument l'ecosistema d'aplicacions orientades a donar suport al mateix procés de *Due Diligence*. Això és pel fet que sembla recomanable usar aquest tipus d'eines en el procés de *Due Diligence* per a mantenir la informació recollida, que és sovint molta i diversa, estructurar-la adequadament i permetre una versió centralitzada de tota la informació acumulada per a tots els participants en el procés en tot moment. Aquestes eines s'han popularitzat en els últims anys i han proliferat diverses versions de diversos fabricants.

2. Aspectes clau d'IT en el procés de la Due Diligence

Certament, són molts i variats els aspectes en els quals gairebé totes les empreses depenen de la tecnologia avui dia. No és l'ànim d'aquest article ser exhaustius en aquest apartat sinó aportar al lector una visió global, clara i concisa, dels principals punts que haurien de ser valorats. En nom de tal claredat classificarem els diferents aspectes en les següents categories:

- **Estructura, Estratègia i Talent del departament de Tecnologia de la Informació.** Especial atenció despertarà l'existència de la funció d'Innovació en el departament reflectida en l'aparició d'un CTO (*Chief Technological Officer*) o potser d'un CDO (*Chief Data Officer*) que ens permeti identificar inequívocament que la companyia compta amb una estratègia a llarg termini per al seu departament d'IT i, per tant, un alineament amb el Pla Estratègic de l'empresa.
  Fonamentalment, l'existència d'aquestes dues figures, CDO i CTO, mereixen una especial atenció per part del responsable de la *Due Diligence*, ja que tant en el control de les dades com de les noves tecnologies poden ser un factor diferencial per a la companyia i tant el talent de les persones que ocupen tals posicions com la seva estratègia a mitjà i llarg termini serien un factor clau per a aconseguir els objectius futurs de l'empresa.
  En aquest punt cobra especial importància la revisió del Pla de Sistemes de l'entitat (a vegades Pla Estratègic de Sistemes) on ha de trobar-se no sols la fórmula per a rendibilitzar els costos d'IT sinó també aquelles tecnologies clau que han d'incorporar-se a futur en el Mapa de Sistemes i que han de permetre no sols el creixement del negoci sinó també, sovint, la mateixa supervivència de l'empresa davant dels competidors directes. L'alineament que el responsable de la *Due Diligence* pugui detectar entre Pla de Sistemes i Pla Estratègic de l'Empresa, així com els diferents comitès establerts entre CEO i IT per a mesurar l'avanç de les tasques i la consecució dels resultats parcials serà un factor rellevant a l'hora de mesurar la importància de les persones, els processos i les eines d'IT en el futur de la companyia.
- **Risc Operacional especialment a tot allò que es refereixi a la continuïtat del negoci i als procediments de *Disaster Recovery* que s'hagin establert**. Aquest és potser l'apartat més tradicional en IT i que engloba aquells aspectes operacionals, tècnics i econòmics relacionats amb la mateixa funció d'IT i que són comunes a la majoria de les empreses modernes:

- Les **llicències i les subscripcions de productes i aplicacions** han d'estar sota control i mai excedir els volums contractats. És cert que molts contractes de fabricants de programari permeten una certa variació respecte a la cosa contractada, però normalment s'esperen regularitzacions periòdiques en cas d'ampliació significativa. Aquí serà rellevant no sols conèixer el contracte de llicències subscrit per les parts sinó a més verificar les últimes factures de compra en el capítol de llicències almenys amb els *partners* tecnològics rellevants. En particular, cal parar esment a les subscripcions de programari on el cost sol anar associat a un *pay per use*. Això és molt habitual en productes desplegats en *cloud* que utilitzen un model de *Software as a Service* (SaaS) com és el cas de la majoria dels productes de Microsoft.
  Un dels principals problemes és l'ús d'usuaris genèrics per a l'accés a aplicacions on un grup d'usuaris comparteix l'accés al servei. Afortunadament, aquesta és una pràctica que s'està abandonant progressivament, ja que a més d'estar específicament prohibit per la majoria dels fabricants, impedeix la deguda traçabilitat de les operacions en el sistema.
- Des de la perspectiva de la continuïtat del negoci, cal parar esment a l'existència d'una implementació **madura dels processos d'ITIL**. La ITIL o *Information Technology Infrastructure Library* és un conjunt de bones pràctiques vastament acceptat entre els professionals d'IT com una forma senzilla i estructurada d'organitzar les operacions IT de l'empresa. La ITIL organitza i regula els principals processos de les operacions IT, com la Gestió del Canvi (*Change*), Incidental (*Incident*), dels Problemes (*Problem*) o el monitoratge (*Event Management*). Especial esment a la gestió de la capacitat (*Capacity Planning*) i configuració (*Configuration*) que, en el cas de tenir mancances en el moment de la *Due Diligence*, significaran un cost d'adaptació posterior.
- L'**obsolescència de la tecnologia** és un altre dels problemes greus que poden aparèixer. En aquest cas, la no implementació de noves versions de maquinari o programari de manera duradora sobre els sistemes de l'empresa pot significar un risc d'obsolescència que el nou propietari haurà d'afrontar tard o d'hora. Aquesta obsolescència, en el cas de no ser esmenada, pot implicar greus problemes de disponibilitat de les aplicacions que afectin el normal desenvolupament del negoci.
- Quant **a la disponibilitat**, cal revisar l'arquitectura dels centres de processament de dades (*Datacenters*) i la disponibilitat teòrica que aporten. Un registre raonable per a les empreses amb sistemes crítics

de negoci seria d'un 99,9% de disponibilitat anual, la qual cosa representa menys de deu hores de caiguda a l'any, normalment descomptant les parades planificades per manteniment o altres raons. Normalment, els professionals que realitzin la *Due Diligence* sol·licitaran els RTOs (*Recovery Time Objective*) per a la recuperació del servei en cas d'incident i els RPOs (*Recovery Point Objective*) per a la recuperació de dades en cada servei crític. Aquests indicadors estan íntimament vinculats als nivells de servei (*Service Level Agreements*) contractats amb els diferents proveïdors i, per tant, un canvi en la disponibilitat global sol necessitar una inversió econòmica que s'ha de conèixer i de calcular durant la *Due Diligence*.

- Finalment, **l'existència de patents o estratègies d'incorporació al mercat** d'un nou producte o servei han de ser mesurades minuciosament analitzant el *business plan* corresponent. Per descomptat, això ocorrerà principalment en empreses l'activitat de les quals estigui relacionada amb la mateixa tecnologia com és el cas de les *start up*s tecnològiques. No és objecte d'aquest article aprofundir en les especials característiques que una *Due Diligence* d'una empresa emergent ha de contemplar, però sembla evident que necessita unes particularitats específiques derivades de la seva particular condició d'empresa "nova" en el mercat i del risc que aquest punt pugui significar.

• **Funcionalitat de les aplicacions i serveis.** Especialment de l'ERP (*Enterprise Resource Planning*) entès com el sistema central (*core*) de la companyia i del CRM (*Customer Relationship Management*) com a plataforma única de relació amb el client requeriran una anàlisi en profunditat per part del responsable del procés de *Due Diligence*. L'existència d'un ERP que agrupi la majoria dels processos de l'empresa, tant en àrees financeres, logístiques o comercials fa d'aquest servei un dels més rellevants de la companyia. El cas del CRM és també rellevant. Se suposa que el CRM concentra tot el coneixement que l'empresa posseeix sobre els seus clients. Des de les seves dades personals i administratives als seus cicles de compres i les seves particularitats operatives, logístiques o tècniques. El CRM és un repositori centralitzat de tota la informació que els diferents executius de vendes necessiten per a poder fer una bona feina. Tots dos sistemes són, per tant, capitals per al funcionament de l'empresa i seran objecte d'estudi particular per part de la *Due Diligence* com a components fonamentals del mapa de sistemes IT.

  En particular i a més de la potencial obsolescència del producte i del seu degut manteniment quant a versions i contractes de manteniment amb el fabricant, s'haurà de revisar l'estructura bàsica de dades pel

que fa a les taules principals i relacions entre elles per a verificar que presenten un disseny funcional adequat i poden respondre a les preguntes o informes que se sol·licitin per part del comprador. Qualsevol manca en aquest aspecte ha d'anotar-se com un *gap* a esmenar que, òbviament, tindrà un impacte econòmic depenent de la gravetat del problema i de les possibles alternatives. És probable que, a més del CRM i de l'ERP, existeixin en el mapa de sistemes de l'empresa altres serveis IT que mereixin igualment aquest tractament especial. El seu nombre i complexitat dependrà de l'empresa, sector, mapa tecnològic i història de la companyia i és difícil de precisar de manera genèrica.

- **Arquitectura Tecnològica.** Revisarem en aquest apartat l'estratègia tecnològica de la companyia: si la seva aposta és ferma cap al *Cloud Computing* i el món del programari com a servei (SaaS) o, per contra, manté una arquitectura híbrida on conviuen els serveis externs amb els desplegaments *onpremise* en els *datacenters* de la companyia. Una estratègia o la contrària pot implicar grans costos recurrents (costos operatius o OPEX) que poden esmorteir-se amb la deguda inversió.

  Un altre capítol rellevant és el de les capacitats d'integració tecnològica de la companyia, sovint oblidades malgrat la seva cabdal importància per al funcionament IT de l'empresa moderna. En aquest cas, és especialment rellevant valorar la capacitat de la tecnologia de l'empresa per a assumir futures operacions de *Merge & Acquisition* a curt o mitjà termini. Si es preveu que aquestes operacions puguin esdevenir, aquest capítol cobra gran rellevància per a la *Due Diligence*, ja que la plataforma tecnològica i els equips de treball IT han d'estar preparats per a assumir-ho. Aquí és important en l'àmbit tecnològic l'existència d'un bus de serveis que aglutini els diferents serveis tecnològics disponibles en una plataforma àgil i senzilla d'usar per a una tercera part que participi en futures integracions dins de futurs escenaris de M&A.

  Finalment, en aquest apartat d'Arquitectura i encara que potser és menys rellevant que els anteriors, no vull deixar d'esmentar la importància de com s'ha abordat en la companyia el tema de la multicanalitat. En concret i si existeixen *apps* desenvolupades *inhouse*, caldria analitzar-ne l'ús i determinar si l'empresa les està usant adequadament per a arribar de la millor manera possible al seu mercat i clients. Un altre punt interessant per a comprovar és si existeix una estratègia de desenvolupament d'aplicacions web en manera *responsive*, entès el terme com a unes aplicacions capaces d'adaptar-se al

dispositiu que les requereixi, sigui aquest un telèfon intel·ligent, una tauleta o un ordinador personal. Si no és així, els costos d'adaptació de tals aplicacions han de ser considerats com un potencial risc després de la compra.

- **Seguretat Informàtica i Ciberseguretat.** Pocs aspectes tan rellevants avui dia com aquest. Aquí, la figura del CISO (*Chief Information Security Office*) i l'existència d'una política de seguretat sòlida i amb el suport de la direcció són fonamentals. Per descomptat, la sensibilitat d'una companyia i l'impacte reputacional que pugui suportar en cas de ciberatac han de ser molt tinguts en compte. Desafortunadament, el *ransomware* ha demostrat ser comú en els nostres dies i difícil de predir o fins i tot de detenir tenint en compte la llarga llista de grans i conegudes empreses i institucions, públiques o privades, que han estat víctimes dels cada vegada més sofisticats *hackers* en el passat recent.

  Per tant, **la ciberseguretat** es converteix en un pilar imprescindible en el funcionament diari de les empreses connectades a la xarxa. Hem de partir de la base que l'única empresa segura cent per cent és avui dia aquella empresa que no està connectada a Internet, la simple connexió amb el món exterior implica un cert risc que cal assumir i comptar després amb les eines que permetin defensar-se dels ciberatacs i dels seus *hackers*. Aquesta circumstància s'ha agreujat després de la crisi de la COVID-19 el març de 2020 amb l'arribada del teletreball massiu. Les eines de videoconferència i missatgeria instantània han evolucionat notablement en els últims dos anys i s'han convertit en la penúltima revolució silenciosa que IT ha aportat a l'empresa. El procés de *Due Diligence* ha de tenir en compte l'estratègia de teletreball en la companyia, no sols per la possibilitat de nous confinaments parcials o fins i tot estrictes (en el pitjor dels casos) sinó també per l'aportació d'aquests mètodes de treball a la conciliació de la vida familiar i a aconseguir, per tant, empleats més satisfets i per això més productius. Per descomptat, la concurrència necessària en termes d'amplada de banda de comunicacions i dispositius mòbils ha de ser objecte d'atenció per a garantir que la contingència potencial serà coberta per la tecnologia disponible arribat el moment.

  L'existència i el seguiment d'un pla de seguretat encaminat a auditar internament els potencials riscos i les vulnerabilitats per a corregir-los amb les degudes implementacions, tant programari com maquinari, són bones pistes per a ajudar a determinar la salut de la seguretat IT de la companyia. Altres aspectes que poden ajudar al responsable de la *Due Diligence* a determinar el grau de maduresa de la seguretat IT

en la companyia és l'existència del que s'ha anomenat "hacking ètic", on els ciberatacs són provocats per un *third party* contractat per la companyia que fa de "hacker" per a trobar vulnerabilitats i alertar al responsable de seguretat per a la seva correcció abans que els *bad boys* del ciberespai ho facin al seu torn. En altres casos, la mateixa companyia ha llançat "hams" de *phishing* entre els seus mateixos empleats per a conscienciar sobre la necessitat d'estar sempre alerta i no atendre a determinats cants de sirena digitals. Aquesta és una pràctica que té els seus detractors, ja que en moltes ocasions aquest *phishing* ètic s'associa a campanyes internes on s'ofereix un premi, simulant al departament de Recursos Humans de la companyia, per exemple, un telèfon intel·ligent, a canvi de contestar una simple enquesta o similar. Aquesta última categoria es coneix també amb Enginyeria Social en algunes empreses.

- ***Data* i Automatització.** En apartats anteriors hem esmentat el *Chief Data Officer* o *CDO* com a figura clau del departament de tecnologia. Efectivament, aquesta figura és el garant intern tant de la qualitat de les dades com del *reporting* proporcionat a les diferents àrees de negoci. No és només una qüestió de forma sinó d'unicitat de les dades i homogeneïtat transversal d'aquestes dades. Aquesta és una qüestió transcendental avui dia per a la presa de decisions així que es converteix en un aspecte per a tenir en compte per part de la *Due Diligence*. Els serveis tecnològics associats a aquest punt i que, per tant, han de ser molt tinguts en compte són els sistemes operacionals, *Data Marts*, *Data Warehouse* i més recentment els *Data Lakes*, i les eines de *Business Intelligence*.

  Potser encara més important que aquesta responsabilitat del CDO és la funció predictiva que l'anàlisi de dades acumulades en els seus sistemes pot (i ha de) proporcionar a les diferents àrees de negoci. En els últims anys, companyies com Facebook o Google han demostrat que existeixen pautes noves en els hàbits de compres dels consumidors. Aquestes tendències, una vegada detectades sobre la base del que anomenem el *Big Data* i convenientment ensinistrades en els sistemes amb tècniques de *Machine Learning* (una de les moltes branques de la intel·ligència artificial) poden significar un nivell superior de vendes futures per a la companyia. Aquestes pautes o tendències són les que el CDO amb els seus *Data Architects* ha de ser capaç de destil·lar de les dades acumulades per la companyia en tota la seva història i canalitzar degudament cap a les àrees de negoci per a certificar la bondat de la predicció. És evident que és una tasca àrdua que requereix inversió, però també és evident que altres empreses pione-

res han recorregut un camí que és aquí per a ser recorregut també. Des del punt de vista de la *Due Diligence*, la maduració d'aquest procés de *Big Data* ha de poder mesurar-se i avaluar-se com un actiu més de l'empresa valorada.

Finalment, i per a tancar aquest capítol de *Data*, ens referirem a l'automatització dels processos operatius o de negoci de la companyia. Si bé és cert que aquesta és una activitat transversal en l'empresa que normalment sol ser liderada per un grup d'Organització fora de la IT, no és menys veritat que el paper de la IT és fonamental en la implementació tècnica i funcional de tot allò que l'Organització pretén. En aquest cas, el professional que realitza la *Due Diligence*, ha de buscar les eines de *Workflow*, també anomenades per les seves sigles en anglès, BPM o *Business Process Management*, que seran les que el duran a entendre fins a quin punt els processos de l'empresa han estat analitzats, com s'han implementat i com s'estan utilitzant per part dels departaments usuaris. Com més processos hagin estat identificats i mecanitzats, més eficient és la companyia.

Per descomptat i per a acabar, hi ha altres formes d'automatització en el camp tecnològic més enllà del BPM. Des dels habituals processos *batch* de càrrega de dades i els serveis web que sincronitzen dades en línia fins a una de les tecnologies que amb més força han tret el cap al mercat de la IT empresarial en els últims anys, el RPA o *Robotic Process Automation*. Dit d'una altra manera, l'ús de robots tecnològics (els *chatbots* que ens atenen ara en molts serveis en línia són un bon exemple) per a simular humans sense que el client ho detecti de cap manera. Aquesta és una tecnologia relativament nova, que ha madurat de manera ràpida en els últims anys i que permet substituir tasques operatives sobre serveis IT realitzats per un usuari per un *robot*. Aquest robot necessita un cert entrenament, però una vegada l'aconsegueix i en teoria, és tan eficient com l'humà, però infinitament més ràpid, de manera que l'eficiència està servida. De nou un apartat a considerar dins de la *Due Diligence*.

En definitiva, la part operacional de qualsevol *Due Diligence* requereix una anàlisi detallada de totes o gairebé de les components IT que hem enumerat en els apartats anteriors. Això pot significar la recopilació i la gestió posterior d'una gran quantitat de dades. És aquí on la tecnologia també aporta solucions per a fer el treball de l'auditor més senzill. Les aplicacions dissenyades específicament per al tractament de *Virtual Data Rooms* s'adapten perfectament a la problemàtica generada durant la *Due Diligence* com veurem en el següent apartat.

3. Aplicacions informàtiques per al Suport al procés de *Due Diligence*

Dins de les innombrables famílies de programari que han aparegut en els últims anys ens interessen especialment per a aquest article aquells productes que poden englobar-se dins de la família de *Vendor Risk Management Tools*.

El procés de *Vendor Risk Management* és responsable d'assegurar que l'ús de serveis externs de la IT proporcionats per altres companyies (*third party*) no ens crearà un inacceptable potencial per a una disrupció del negoci o impacte negatiu en el rendiment del negoci. Aquestes aplicacions ajuden al monitoratge, la gestió i l'assessorament de determinats processos crítics d'IT o per a la IT, gestionant alhora l'exposició al risc i aportant uns indicadors per a controlar aquest risc. En general s'associen a tot el relacionat amb el compliment normatiu (*Compliance*) de l'empresa moderna. La majoria han desenvolupat uns mòduls específics per al control i seguiment de la *Due Diligence*. La facilitat per a crear *Virtual Data Rooms* basats en espais en *cloud* que compten amb la deguda facilitat és una altra de les característiques fonamentals d'aquestes aplicacions.

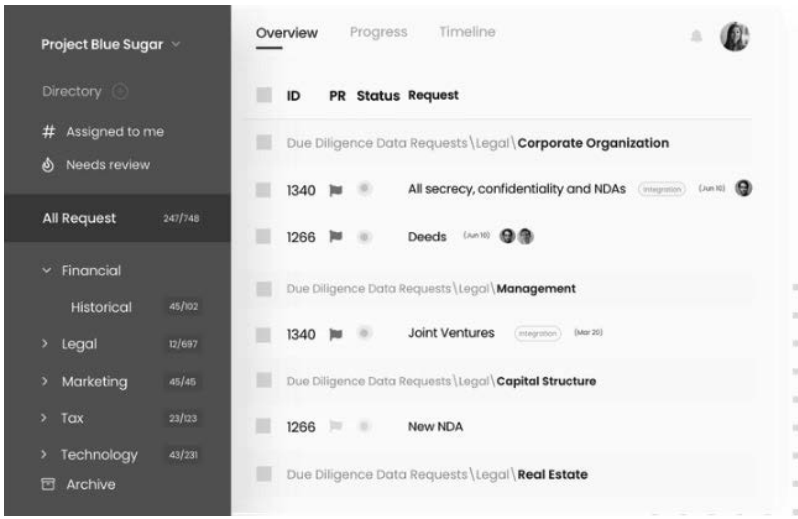
En general es tracta d'aplicacions de propòsit específic l'objectiu del qual és minimitzar l'esforç necessari i maximitzar el temps per a l'anàlisi. El propòsit és fugir d'un procés focalitzat en un conjunt poc estructurat de correus, PDF, Word i Excel units per un únic document mestre realitzat, al seu torn, amb una altra eina microinformàtica com Word o Power Point. Per descomptat aquesta manera de treballar no és la més adequada a causa de la ingent quantitat de dades que es manegen durant els processos de *Due Diligence*.

Una molt millor solució és disposar d'un programari dissenyat específicament per a la *Due Diligence* que guii a través del procés de principi a fi. Això facilitarà la compartició de formularis, *checklists* i qualsevol altre contingut. En general, un procés de *Due Diligence* és seqüencial i ordenat, per la qual cosa des d'un punt de vista funcional pot resumir-se en una llista de tasques ordenada. El format de *checklist* on cada tasca de la llista queda convenientment marcada una vegada completada proporcionarà el suport perfecte al procés. D'aquesta manera i comptant amb alguna d'aquestes eines des del principi, és possible monitorar, controlar i informar del progrés de les tasques en qualsevol moment i amb la garantia que l'actualització és òptima.

En molts casos, aquestes eines incorporen fluxos de treball (o *workflows*) que permeten una mínima i simple programació de passos (*steps*) i autoritzacions (*grants*) per a aconseguir la confluència de totes les parts implicades en un mateix frontal sobre una base de dades comuna per a acabar amb els emails i altres tipus d'incòmoda informació poc estructurada.

Al lector àvid d'un detall més gran en aquest camp no li serà gens difícil després d'una ràpida cerca a Internet, descobrir bons exemples d'aquesta mena d'aplicacions. En general, totes les eines que es poden trobar a Internet estan lligades al món del *Compliance* i, com ja hem dit, tecnològicament incorporades en la família de productes associats al *Vendor Risk Management*.

En la següent Figura 1, pot veure's com a exemple l'aparença d'una d'aquestes aplicacions amb el característic *checklist* ja comentat i un senzill codi de colors (semàfor) que permet a primera vista una impressió del grau d'avanç de la tasca avaluada.



Font: www.dealroom.net

Figura 1. Exemple de *check list.*

4. Conclusions

La component operacional de la *Due Diligence* és un procés exhaustiu de recerca de la companyia objecte que ha de definir com ho fa primer i com de bé ho fa després. La intersecció d'aquest procés amb la tecnologia sobre la qual la companyia desplega els seus processos de vendes i operatius és inevitable si es desitja un producte final complet.

La majoria dels aspectes tecnològics (Ciberseguretat, Mapa i Pla de Sistemes, Infraestructura, Arquitectura i aplicacions, etc.) són comuns a gairebé qualsevol empresa i hauran de ser tractats per l'expert IT dins de

l'equip responsable de la *Due Diligence*. Aquest expert serà el responsable d'avaluar els aspectes clau de la IT per a la *Due Diligence* i valorar els possibles riscos que puguin existir.

Cada companyia tindrà les seves pròpies particularitats que faran cada *Due Diligence* diferent de les anteriors. Aquesta diversitat fa recomanable comptar amb aplicacions desenvolupades específicament per a donar una estructura a un procés que pot arribar a ser fàcilment difícil de manejar.

Referències bibliogrèfiques

Blokdyk, G. (2020) "Vendor Risk Management Practices: A Complete Guide". Ed. Emereo Publishing.

Dewey, R. (2018) "Valuing Data: An Open Framework". Ed. CRC Press.

Langer, A. M. (2018) "Strategic Information Technology: Best Practices to Drive Digital Transformation". Ed. Wiley.

Small, M. J. (2019) "A Quick Guide to Understanding IT Security Basics for IT Professionals". Ed. RMS Consulting.

Soisco, M. (2015) "IT Due Diligence: merger and acquisition discovery process". Ed. MDE Enterprises.