

Ръководство и управление на информационните технологии в предприятията на основата на COBIT 2019

Валери Дикльовски*

Резюме: В светлината на дигиталната трансформация информационните технологии (IT) станаха решаващи за подкрепата, устойчивостта и растежа на предприятията. Създаването на стойност на заинтересованите страни (т.е. осъзнаване на изгодата при оптимална цена на ресурсите, докато се оптимизира рискът) често се задвижва от висока степен на дигитализация в нови бизнес модели, ефективни процеси, успешните иновации и т.н. Дигитализираните предприятия са все по-зависими от IT за оцеляване и растеж. Като се има предвид централността на IT за ръководството на корпоративния риск и генерирането на стойност, през последните три десетилетия се отделя специално внимание на корпоративното управление на информационните технологии (Enterprise Governance of Information Technology – EGIT). EGIT е неразделна част от корпоративното управление. През годините са разработени и популяризирани рамки за най-добри практики, които да подпомогнат процеса на разбиране, проектиране и прилагане на EGIT. COBIT е рамка за ръководството и управлението на информационни-

те технологии на предприятието. COBIT® 2019 награжда и интегрира повече от 25 години развитие в тази област, като не само включва нови знания от науката, но и като привежда тези прозрения в оперативни практики. Разгледани са характеристиките и структурата на COBIT, както и нововъведенията в тази версия на рамката. Представени са и принципите за създаване на бизнес казус за ефективно прилагане на COBIT като подход за подобряване на управлението на информационните технологии в корпоративна среда.

Ключови думи: управление, информация, технологии, EGIT, COBIT.

JEL: M15, M42.

1. Увод

Корпоративното ръководство на информационните технологии е сложно и многостранно. Няма общоприет, стандартизиран идеален начин за проектиране, внедряване и поддържане на ефективен EGIT в рамките на една организация. Като такива, членовете на управителните съвети и висшето ръководство трябва да приспособят своите EGIT мерки и да прилагат своите собствени специфични характеристики и нужди. Те трябва също така да са готови да приемат по-голяма отговор-

* Валери Дикльовски е докторант в катедра „Финансов контрол“ на УНСС.

ност за ИТ и да използват различно мислене и култура за осигуряване на стойност от ИТ (Weill & Ross, 2004; Haes & Grembergen, 2004).

Управлението на ИТ е отговорност на борда на директорите и изпълнителния мениджмънт. Той е неразделна част от управлението на предприятието и се състои от ръководството и организацията на структури и процеси, които гарантират, че ИТ организацията поддържа и разширява стратегията и целите на организацията. ИТ управлението е организационният капацитет, упражняван от борда, изпълнителното ръководство и ИТ управление за контрол на формулирането и прилагането на ИТ стратегията за сливане на бизнес и ИТ (Haes & Grembergen).

2. Ръководство и управление на информацията и технологиите

EGIT (Enterprise Governance of Information Technology) се занимава с постигането на стойност от дигиталната трансформация и намаляването на бизнес риска, произтичащ от дигиталната трансформация (Haes & Grembergen). По-конкретно, след успешното приемане на EGIT могат да се очакват три основни резултата:

- Реализация на ползите – създаване на стойност за предприятието чрез ИТ, поддържане и увеличаване на стойността, получена от съществуващите инвестиции в ИТ, и премахване на ИТ инициативи и активи, които не създават достатъчна стойност. Основният принцип на ИТ стойността е навременното и в рамките на бюджета предоставяне на подходящи услуги и решения, които генерират предвидените финансови и нефинансови ползи. Стойността, която ИТ предоставя, трябва да бъде пряко приведена в съответствие

със стойностите, върху които е фокусиран бизнесът. Освен това, ИТ стойността трябва да се измерва по начин, който показва въздействието и приноса на инвестициите, станали възможни с подкрепата на ИТ, в процеса на създаване на стойност на предприятието (В този текст ИТ се използва по отношение на организационния отдел с основна отговорност за технологиите. ИТ, използван в този текст, се отнася до цялата информация, която предприятието генерира, обработва и използва за постигане на своите цели, както и технологията за поддръжка в предприятието).

- Оптимизация на риска – това включва адресиране на бизнес риска, свързан с използването, собствеността, експлоатацията, участието, влиянието и приемането на ИТ в предприятието. Бизнес рискът, свързан с ИТ, се състои от събития, свързани с ИТ, които биха могли да повлияят на бизнеса. Докато предоставянето на стойност се фокусира върху *създаването* на стойност, управлението на риска се фокусира върху *запазването* на стойността. Управлението на риска, свързан с ИТ, трябва да бъде интегрирано в подхода за управление на риска на предприятието, за да се осигури съсредоточаване на предприятието върху ИТ. Той също трябва да бъде измерван по начин, който показва въздействието и приноса на оптимизирането на свързания с ИТ бизнес риск върху запазването на стойността.
- Оптимизация на ресурсите – това гарантира, че са налице подходящи възможности за изпълнение на стратегическия план и са осигурени достатъчни, подходящи и ефективни ресурси. Оптимизация на ресурсите гарантира, че се предоставя една интегрирана,

икономична ИТ инфраструктура, че е въведена нова технология, съгласно изискванията на бизнеса, и че остарелите системи са актуализирани или поменени. Тъй като признава важността на хората, в допълнение към хардуера и софтуера, вниманието се съсредоточава върху осигуряване на обучение, насърчаване на задържането и гарантиране на компетентност на ключовия ИТ персонал. Важен ресурс са данните и информацията, а използването на данни и информация за получаване на оптимална стойност е друг ключов елемент на оптимизацията на ресурсите.

В голямо проучване на международна авиокомпания, демонстрираните ползи от EGIT включват: по-ниски разходи за непрекъсваемост, повишен капацитет за иновации, повишаване на синхрона между цифрови инвестиции и бизнес цели и стратегии, увеличено доверие между бизнеса и ИТ и преминаване към „ценностно мислене“ около цифровите активи, и всичко това благодарение на ИТ.

Изследванията показват, че предприятията с лошо проектирани или възприети подходи към EGIT се представят по-лошо в хармонизирането на бизнеса и ИТ стратегиите и процесите. В резултат на това е много по-малко вероятно такива предприятия да постигнат планираните бизнес стратегии и да реализират бизнес стойността, която очакват от дигиталната трансформация (Gerow, Thatcher & Grover, 2015, 465-491).

От това става ясно, че управлението трябва да бъде разбрано и приложено много извън често срещаната (т.е. тясната) интерпретация, предложена от съкращението за управление, риск и съответствие (GRC). Самото съкращение GRC имплицитно предполага, че съответствието

и свързаният риск представляват спектъра на управлението.

3. COBIT

COBIT е рамка за ръководството и управлението на информационните технологии на предприятието, насочени към цялото (Haes, Grembergen, Joshi & Huygh, 2019). Корпоративни ИТ означава цялата технология и обработка на информация, които предприятието въвежда за постигане на своите цели, независимо от това къде се случва това в предприятието. С други думи, ИТ на предприятието не е ограничено до ИТ отдела на организация, но със сигурност го включва.

Рамката COBIT прави ясно разграничение между ръководство и управление. Тези две дисциплини обхващат различни дейности, изискват различни организационни структури и служат за различни цели. Ръководството гарантира, че: нуждите, условията и опциите на заинтересованите страни се оценяват, за да се определят балансираните и съгласувани цели на предприятието; посоката е зададена чрез определяне на приоритет и вземане на решения; изпълнението и съответствието се контролират според договорените насоки и цели.

В повечето предприятия цялостното ръководство е отговорност на съвета на директорите под водачеството на председателя. Специфични отговорности на ръководството могат да бъдат делегирани на специални организационни структури на съответното ниво, особено в по-големи, сложни предприятия. Управлението планира, изгражда, внедрява и следи дейностите, в съответствие с посоката, зададена от ръководния орган, за постигане на целите на предприятието. В повечето предприятия управлението е отговорност на изпълнителното ръководство под водаче-

ството на главния изпълнителен директор (СЕО).

СОВИТ определя компонентите за изграждане и поддържане на система за ръководство: процеси, организационни структури, политики и процедури, информационни потоци, култура и поведение, умения и инфраструктура.

СОВИТ определя факторите на проектиране, които трябва да се вземат предвид от предприятието за изграждане на най-подходяща система за ръководство.

СОВИТ се занимава с проблемите за ръководство чрез групиране на съответните компоненти в целите на ръководството и управлението, които могат да бъдат управлявани до необходимите нива на дееспособност.

СОВИТ не е пълно описание на цялата ИТ среда на предприятието. СОВИТ не е рамка за организиране на бизнес процеси. СОВИТ не е техническа рамка за управление на всички технологии.

СОВИТ не взема и не предписва решения, свързани с ИТ. Тя няма да реши коя е най-добрата ИТ стратегия, каква е най-добрата архитектура или колко може или трябва да струва ИТ. По-скоро СОВИТ определя всички компоненти, които описват кои решения трябва да бъдат взети и как и от кого трябва да бъдат взети (Haes, Grembergen, Joshi & Huugh, 2019).

4. СОВИТ 2019

СОВИТ® 2019 е по-добър спрямо предишните версии на СОВИТ в следните области:

- Гъвкавост и отвореност – определянето и използването на проектните фактори позволява СОВИТ да бъде пригоден за по-добро съгласуване с конкретен контекст на потребителя. Отворената архитектура на СОВИТ дава възможност за добавяне на нови проблемни области или

промяна на съществуващи, без преки последици за структурата и съдържанието на основния модел на СОВИТ.

- Валидност и приложимост – Моделът СОВИТ поддържа съотнасяне и привеждане в съответствие с концепции, произхождащи от групи източници (например, най-новите ИТ стандарти и регламенти за съответствие).
- Предписателна приложимост – Моделите като СОВИТ могат да бъдат описателни и предписателни. Концептуалният модел на СОВИТ е конструиран и представен така, че неговото създаване (т.е. прилагането на адаптирани компоненти за ръководство на СОВИТ) се възприема като рецепта за персонализирана система за ръководство на ИТ.
- Управление на ефективността на ИТ – Структурата на модела СОВИТ за управление на ефективността е интегрирана в концептуалния модел. Концепциите за зрялост и способности са въведени за по-добро привеждане в съответствие с CMMI (<https://cmmiinstitute.com/>).

5. Създаване на бизнес казус за анализ и обосноваване на изпълнението на EGIT

Всяко предприятие има свои причини за подобряване на EGIT и собствен подход към подготовката на бизнес казуси. Този пример и указанията в тази публикация са предоставени, за да подпомогнат съсредоточаването върху въпросите, които трябва да бъдат разгледани в бизнес казус.

Примерният сценарий се отнася за Корпорация "X", голямо мултинационално предприятие със смесица от традиционни, утвърдени бизнес единици, както и нов бизнес, базиран на Интернет, възприемащ най-новите технологии. Много от бизнес звената са придобити и съществуват в различни страни с различна местна поли-

тическа, културна и икономическа среда. Екипът на изпълнителното ръководство на централната група е бил повлиян от новите указания на ръководството на предприятието, включително COBIT, които те са използвали централно за известно време. Те искат гаранции, че бързото разширяване и приемането на усъвършенствани ИТ ще осигурят очакваната стойност; всички те имат намерение да управляват значителен нов риск. Следователно, те са наложили приемането на единен подход на EGIT в рамките на цялото предприятие. Този подход включва участие на функциите на одита и на риска и вътрешногодишното отчитане от ръководството на бизнес единицата за адекватността на контрола във всички бизнес единици. Въпреки че примерът е извлечен от реални ситуации, той не отразява конкретно съществуващо предприятие.

Програмата EGIT ще се изпълнява в две отделни фази. Първата фаза е фаза на развитие, в която екипът ще развива и изпробва подхода и набора от инструменти, които ще се използват. В края на фаза 1 резултатите ще бъдат представени на управлението на групата за окончателно одобрение. След като се достигне окончателното одобрение, във формата на одобрен бизнес казус, програмата EGIT ще бъде въведена в цялото предприятие по съгласуван начин (изпълнение, фаза 2).

Бордът на директорите, подпомаган от комисиите по риск и одит, ще гарантира, че ефективността на EGIT на групата се оценява, наблюдава, докладва и разкрива в декларацията на EGIT като част от интегрирания годишен доклад на предприятието. Декларацията ще се основава на доклади, получени от екипите по риска, съответствието и вътрешния одит и от управлението на всяко важно дъщерно дружество. Тя ще предостави както на вътрешните, така и на външните заинтересовани стра-

ни една точна и надеждна информация за качеството на ефективността на изпълнението на EGIT.

Службите за вътрешен одит ще предоставят гаранция на ръководството и на одитната комисия за адекватността и ефективността на EGIT.

Бизнес-рискът, свързан с информационните технологии, ще бъде докладван и обсъден като част от процеса на управление на риска в регистрите на риска, представени на съответната комисия по риска. Поради широкото разпространение на ИТ и темповете на промяна на технологиите, е необходима надеждна рамка за адекватен контрол на цялата ИТ среда и за избягване на пропуските в контрола, които могат да излагат предприятието на неприемлив риск. Намерението не е да се възпрепятстват ИТ операциите на различните оперативни единици. Вместо това, трябва да се подобри рисковият профил на звената по начин, който има бизнес смисъл и осигурява повишено качество на услугите и ефективност, като същевременно изрично се постига съответствие не само с EGIT групата на Корпорация "X", но и с всички други законодателни, регулаторни и/или договорни изисквания.

Някои примери за вероятни слаби точки включват:

- Усложнени усилия за осигуряване на ИТ качество поради предприемаческия характер на много от бизнес звената;
- Сложни ИТ операционни модели поради използваните бизнес модели на Интернет услуги;
- Географски разпръснати звена, съставени от различни култури и езици;
- Децентрализираният/федеративен и до голяма степен автономен модел на бизнес контрол, използван в рамките на групата;
- Прилагане на разумни нива на управление

Икономически теории

на информационните технологии в условията на високо техническа и понякога нестабилна ИТ работна сила;

- ИТ балансиране на стремежа на предприятието за иновационни възможности и гъвкавост на бизнеса с нуждата от управление на риска и наличието на адекватен контрол;
- Задаване на нива на риск и толеранс за всяка бизнес единица;
- Нарастваща необходимост от съсредоточаване върху спазването на регулаторните (поверителност) и договорните (платежни карти PCI) изисквания за съответствие;
- Редовни констатации на одита относно слаб ИТ контрол и отчетени проблеми, свързани с качеството на ИТ услугата;
- Успешно и навременно предоставяне на нови и иновативни услуги на силно конкурентен пазар.

Не е необходимо COBIT да се прилага в своята цялост; трябва да се прилагат само тези области, свързани с конкретната гъщерна или бизнес единица, като се вземе предвид следното:

1. Етапът на развитие на всяко звено в жизнения цикъл на бизнеса;
2. Бизнес целите на всяко звено;
3. Значението на ИТ за бизнес единицата;
4. Бизнес риск, свързан с ИТ, с който се сблъсква всяко предприятие;
5. Правни и договорни изисквания;
6. Всякакви други уместни причини.

Ако определено гъщерно гружество или бизнес единица вече е приложило друга рамка или се планира внедряване в бъдеще, прилагането трябва да бъде съотнесено към COBIT за целите на отчитане, одит и яснота на вътрешния контрол.

6. Заключение

COBIT е рамка за ръководството и управлението на информационните технологии на

предприятието, насочени към цялото предприятие. COBIT 2019 акцентира върху гъвкавост и отвореност, приложимост и съответствие с най-новите ИТ стандарти, предписателна приложимост, управление на ефективността на ИТ. Очакваните ползи от прилагането му включват резултати като създаване на стойност за предприятието чрез ИТ, поддържане и увеличаване на стойността, получена от съществуващите инвестиции в ИТ, и премахване на ИТ инициативи и активи, които не създават достатъчна стойност; адресиране на бизнес риска, свързан с използването, собствеността, експлоатацията, участието, влиянието и приемането на ИТ в предприятието; оптимизация на ресурсите, т.е. икономична ИТ инфраструктура, въвеждане на нови технологии, съгласно изискванията на бизнеса, актуализация и подмяна на остарелите системи.

Цитирани източници:

- Gerow, J.E., Thatcher, J.B., & Grover, V., 2015. Six types of IT-business strategic alignment: an investigation of the constructs and their measurement. *European Journal of Information Systems*, 24(5), 465-491.
- Haes, S.D., & Grembergen, W.V., 2004. *IT Governance and Its Mechanisms*. Information Systems Audit and Control Association.
- Haes, S.D., & Grembergen, W.V., 2015. Enterprise Governance of IT. In *Management for Professionals*. Springer.
- Haes, S.D., Grembergen, W.V., Joshi, A., & Huygh, T., 2019. COBIT as a Framework for Enterprise Governance of IT. In *Enterprise Governance of Information Technology*. Springer, Cham.
- Héroux, S., & Fortin, A., 2018. The moderating role of IT-business alignment in the relationship between IT governance, IT competence, and innovation. *Information Systems Management*, 35(2), 98-123.

Weill, P., & Ross, J.W., 2004. *IT Governance: How Top Performers Manage IT Decision Rights* | *for Superior Results*. Harvard Business Press.
<https://cmmiinstitute.com/>