envative
SMARTER SOFTWARE SOLUTIONS
WEB MOBILE IoT

WhitePaper: The Value of Technology Code Reviews Prior to Acquisitions or VC Investments

By Craig Lamb

For code reviews performed as part of investment or M&A due diligence, recognize what type of code review will be conducted, and why. Typically, the focus is on the future state and ability of the software (and team) to execute on the investor's or acquirer's thesis and the product's roadmap. For this reason, a code review is normally conducted as just a part of a holistic IT due diligence assessment that covers more than only the code.

There are many drivers that may necessitate a software code review and it can be performed by manual or automated inspection, or both. Here is a non-exclusive list of reasons for an IT due diligence and/or code review, and a brief on the process:

1) Software Architecture, Scalability, & Extensibility - performed by experienced software architects to look for risks associated with how software was designed and developed. These software auditors may be looking for indications including:

- appropriateness of software architecture paradigms (i.e. single-tier vs multi-tier architecture)
- architecture's ability to vertically and/or horizontally scale
- use of contemporary technology stacks
- platform's ability to scale alongside growth in user adoption or expansion in functionality
- ability to integrate with partner platforms

2) Exposure to Third-Party Platforms - an investor may enlist a code review to assess if the software has an over-dependence on a third-party proprietary platform, which may unveil that the product is more of a value-added reseller. The assessment may include interviews with a technology platform partner if tight integration with the platform is in place.

3) Information Security / Compliance Review - an assessment of the platform's approach to information security, covering threats from both external and internal sources, access and permission management, security for data-in-transit and data-at-rest, approach to application and network penetration testing; may also be performed to assess the company's ability to meet industry compliance standards such as PCI (Payment Card Security), ISO27001 (Standard for Information Management System), HIPAA (Health Insurance Portability and Accountability Act), NIST (National Institute of Standards and Technology), and others.

4) I.P. Valuation - an objective review of the software's "secret sauce" and whether it meets the investor's expectations of propriety; this may involve a high-level code review or 'guided tour' of the code by the software engineers or software architects and a demonstration by product experts. Valuation may be performed by estimating the cost of development.

5) Substandard IT Performance - the software may not be performing as expected or employee turnover may be an issue, and non-technical C-level leaders or board may call for an independent IT assessment. This may be a contentious situation whereby the qualifications of technology leaders may be called into question and also hint at significant exposure to key-man risk.

6) Open-Source Licensing Risk Exposure - open source software can have strict limitations on its use in a proprietary product. As a technology manager, proactive sell side due diligence, even in a light-weight form, to identify, inventory, assess, and, when necessary, remediate open source risks helps ensure the target company receives the best value for its products in an M&A event (and avoid lawsuits).

7) Intellectual Property / Patent Evaluation - often conducted as part of an IP or patent dispute. IT Due Diligence firms are often called upon to perform a low-level inspection and comparison for patent infringement. A popular method to evaluate whether software has been copied is the Abstraction-Filtration-Comparison (AFC) test, and there are software vendors that offer tools to aid in this type of software forensic analysis.

8) IT Spin Out - When a company or private equity firm intends to "spin" or "carve" out one or more business units from a larger organization, a feasibility assessment may be performed to understand the factors associated with detaching the technology assets. Specialized transition management consultants are often hired to perform an IT assessment and assist with the carve out. This type of deal may be especially challenging as it involves on-going management the business along with the transition of people, processes, and technology. The target unit may be tightly integrated and dependent on many of the larger company's resources like data centers, back office accounting and finance systems, customer relationship management software, and more.

The investor or acquirer often enlists an IT due diligence team with a structured process and experienced software architects with subject matter expertise in the appropriate vertical. This reduces the time to come up to speed on the product and ensures that the focus is on only those technology risk items relevant to the business and product's stage in its life cycle. If your company is the subject of an IT assessment, assume the due diligence team will come prepared and interested in learning about your company.

Remember, the process is not about poking holes in a business's or entrepreneur's code, but more about helping to validate the go-forward plan. Especially in the case of an early stage company, it is important for the target to foster a collaborative process, be prepared to explain decisions on trade-offs between cost and time-to-market, be transparent about skeletons in the closet (read: no software has 100% uptime and is without bugs), and provide an IT roadmap that mitigates those risk items, where appropriate. The target company should bring to the process an established and well thought out go-forward plan and be able to explain where the company or product currently stands, and the result will likely be an IT assessment that merely validates the plan and reasons the company seeks investment.

The first step in the process is almost always an information request for IT documentation, diagrams, lists of components and libraries, and/or access to the software code repository.

About Us:
Envative has been in the technology industry for over 20 years providing web, mobile and IoT software development services to "start-ups" and well-established companies across all industries. We are also partnered with Robin Hood Venture Group, an angel investor team out of Philadelphia, performing technical assessments as part of their investment opportunity evaluation process.

About the Author:
Craig Lamb

Craig Lamb is a co-founder and serves as Chief Information Officer at Envative, a software development company offering custom end-to-end solutions in web, mobile and IoT. With over 25 years of experience in Information Technology leadership, he is a researcher and promoter of new technologies that are leveraged in Envative's custom development efforts. Craig's expertise and keen insights have made him a respected leader and an engaging speaker within the tech industry. His greatest source of professional achievement, however, is on the consultative and technologically advanced business culture that he (along with his business partner, Dave Mastrella) has built and cultivated for more than two decades.