



OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: FFIEC Guidance

Description: Risk Management for the Use of
Free and Open Source Software

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel

The Federal Financial Institutions Examination Council has released the attached guidance, “Risk Management for the Use of Free and Open Source Software.” This interagency guidance reviews the risks and controls associated with the use of free and open source software (FOSS).¹ The guidance describes this category of product as software that may be implemented, studied, modified, and distributed without the payment of licensing fees. The adoption and use of FOSS by banks is increasing, and effective controls are required to manage the attendant strategic, operational, and legal risks.

Fundamentally, the risks associated with FOSS are similar to those presented by proprietary or self-developed software. However, distinctive risk management practices connected with the use of FOSS do exist, and bank management should be familiar with them.

National banks should refer to this guidance when they are considering using or deploying FOSS regardless of whether it will be provided internally or by a third-party service provider. The OCC expects national banks to assess the risks to themselves and to their customers, and to implement appropriate risk management processes. The guidance addresses many technical issues, and may require information technology expertise to follow them. Examiners will use this guidance to evaluate the effectiveness of FOSS risk management practices in banks and third-party service providers.

For further information on technology risk management guidance, visit the OCC’s Internet Web site at www.occ.treas.gov.

For questions regarding this bulletin, please contact the OCC’s Bank Information Technology Division at (202) 874-4740.

Mark L. O’Dell
Deputy Comptroller for Operational Risk

Attachment: FFIEC Guidance (Go to: www.fdic.gov/news/news/financial/2004/FIL11404a.html)

¹ The use of the word “free” in this context does not necessarily mean that the software is available at no cost. For additional information about FOSS, refer to www.fsf.org and www.opensource.org.